skillsoft

Percipio Security and Infrastructure Overview for US and EU Deployment Locations

TABLE OF CONTENTS

REVISION HISTORY

VERSION	DATE	AUTHOR	DESCRIPTION
1.0	11/6/2023	Carl Johnson	Created
1.1	12/13/2023	Carl Johnson	Updated vulnerability management timelines to specify units. Added SOC2-Type 1 Certification. Added TX-RAMP.
2.0	02/26/2024	Carl Johnson	Added capabilities to Appendix A regarding phishing, DMARC, and threat intelligence. Added Appendix C with Privacy Notice link.
2.1	05/01/2024	Carl Johnson	Added SOC2 Type 2, Static Code Analysis, and Open-Source tooling to Appendix A Checklist. Added Appendix C.
2.2	08/27/2024	Carl Johnson	Update CE Certificate Links.
2.3	12/10/2024	Carl Johnson	Updated IRAP status, FedRAMP Rev 5 and Key Management.

3.0	02/27/2025	Carl Johnson	Updated IRAP sections.
3.1	07/07/2025	Carl Johnson	Updated Appendix A.

This document replaces all previous variants with the names listed below:

- “Percipio Product Document – Vx.x.pdf”
- “Cloud_Ops_Services_Percipio_US_AWS.pdf”
- “Cloud_Ops_Services_Percipio_EU_AWS.pdf”

NDA NOTICE

This document does not contain any content that requires an NDA to be signed.

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

- Firewall-related hardware, software, or settings
- Intrusion Detection System (IPS)-related hardware, software, or settings
- Network penetration testing
- Vulnerability scanning
- Network topology
- Internal IP scheme
- Operating Systems configuration and security settings
- Software vendors and version in use

INTRODUCTION

This document has been created to provide a high-level overview of the application, infrastructure, and security measures that we have in place to protect your data and ensure the availability and integrity of our systems.

We have invested heavily in our security infrastructure and have implemented advanced security technologies and best practices to ensure that your data is always protected. Our security measures are regularly reviewed and updated to stay ahead of emerging threats and provide the highest level of protection.

We believe that transparency and open communication are essential in building a trusted relationship with our clients, and this document reflects our commitment to transparency and accountability. We hope this document will help you understand the measures we have in place to protect your data and give you confidence in our ability to provide secure and reliable services.

PERCIPIO APPLICATION DESCRIPTION

Skillsoft's AI-driven online learning platform empowers organizations to identify and measure skill proficiencies to ensure their workforce stays relevant. The platform makes skilling personalized and accessible, offering a blend of self-paced courses, hands-on practice, virtual, live, instructor-led classes, and coaching to close skill gaps. And it's available anytime, anywhere, on any device.

- **Help your organization stay competitive and poised for innovation** with expertly curated skilling pathways and measure skills gained over time.
- **Inspire and motivate teams** with AI-driven recommendations, offering relevant assets and experiences based on each learner's role, interests, and behaviors.
- **Customize the experience** to achieve the strategic outcomes of your business. Design and assign live and on-demand skilling experiences with your content or from other providers.
- **Offer learning in daily-use tools and technology** — Seamlessly integrate transformative learning experiences with your current technology without reinventing the wheel.

The Percipio platform includes Coaching and Compliance.

PERCIPIO ARCHITECTURE

AWS WELL ARCHITECTED FRAMEWORK

Percipio was developed using the AWS Well Architected Framework described at the following URL:

https://aws.amazon.com/architecture/well-architected/?wa-lens-whitepapers.sort-by=item.additionalFields.sortDate&wa-lens-whitepapers.sort-order=desc&wa-guidance- whitepapers.sort-by=item.additionalFields.sortDate&wa-guidance-whitepapers.sort-order=desc

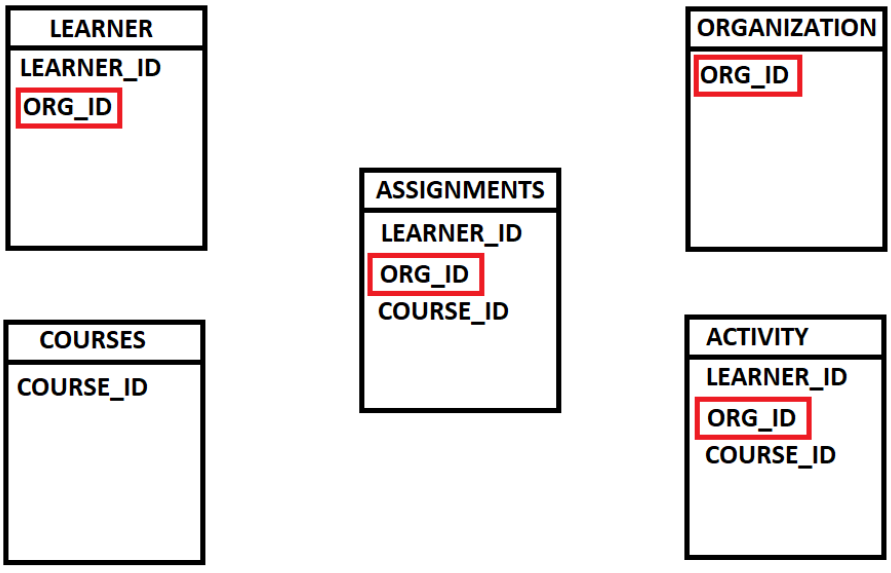
Percipio is designed to be a fault tolerant, rapidly scalable solution that provides predicably reliable delivery of training services.

- Load balancing at the network, internetwork, content delivery network, DNS (Domain Name System), and the application layer provides a resilient, redundant, and reliable service.
- Server hosts use hardened Center for Internet Security (CIS) approved images to ensure reliability and security of the server hosting environments.
- Full data path encryption ensures all information that is sent from the learner to Percipio, and back to the learner is encrypted with Transport Layer Security (TLS) 1.2 and above, and all known weak cryptographic ciphers are removed from service.

- Data encryption is used for all information stored (including backups) in the Percipio environment and leverages the Advanced Encryption Standard in Galois Counter Mode with 256bit keys (AES-256 GCM).
- Use of Route53 enhances reliability and fault tolerance of the Percipio solution.
- Code and Infrastructure production, promotion and release are governed with a rigid Infrastructure as Code system development practice.

SECURE MULTI-TENANT ARCHITECTURE

Percipio is a multi-tenant platform, and customers are logically separated using a tenant key. Below is a simplified diagram illustrating the use of the tenant key.

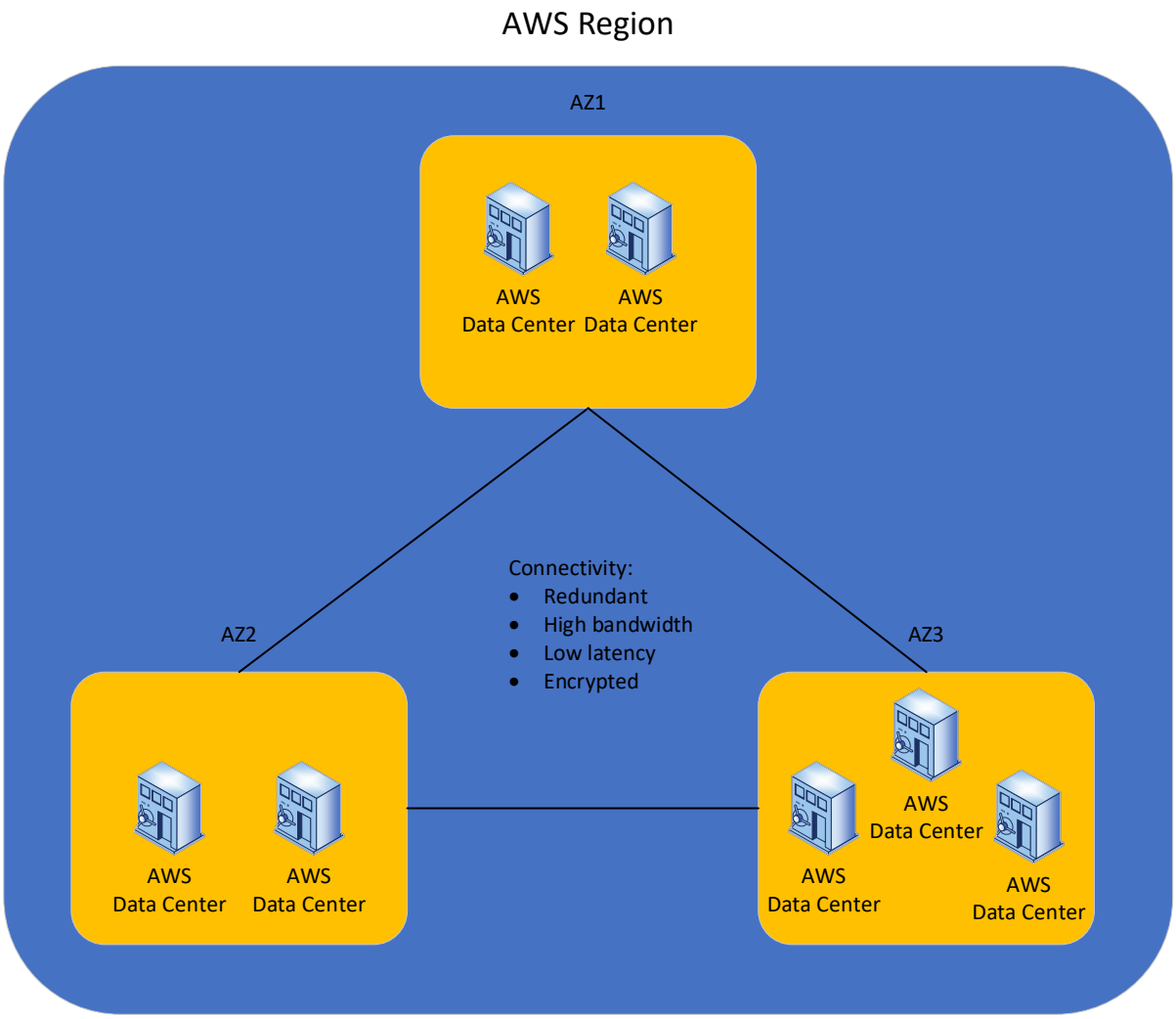


*TENANT KEY SHOWN HIGHLIGHTED IN RED

PERCIPIO HOSTING ENVIRONMENT

PUBLIC CLOUD

The Percipio platform is hosted in a secure and scalable cloud environment. Skillsoft utilizes Amazon Web Services (AWS) as its primary cloud provider for Percipio. AWS offers a world class infrastructure that ensures high availability, scalability, and performance of the platform. Percipio takes advantage of multiple Availability Zones (AZs) within an AWS region. Our use of AZs decreases the likelihood of needing to declare a disaster and fail-over to another AWS region. The relationship between Regions and Availability Zones is illustrated in the diagram below.



The table below gives example scenarios of AZ protection vs. Disaster Recovery (Regional) Protection:

AZ PROTECTION – SCENARIOS	DR PROTECTION – SCENARIOS
• Loss of network connectivity to a datacenter due to construction • Mass hardware failures due to heat, water, etc. • Datacenter facility fire/intentional or accidental activation of fire suppression system • Chemical spill • AWS service failures affecting a facility (intermittent or prolonged)	• Power grid failure • Environmental disaster • Civil unrest • Extreme weather event • AWS service failures that are regional • Workforce interruptions

The hosting environment is designed to meet the highest security standards and compliance requirements. Skillsoft implements various security measures, such as data encryption, access controls, intrusion detection and prevention, and regular security audits and assessments, to protect user data and ensure the platform's integrity.

The platform is also designed for optimal performance and scalability. The platform can handle many concurrent users and can scale up or down dynamically based on usage patterns.

Percipio deployment locations are seen in the table below with RTO and RPO commitments:

DEPLOYMENT LOCATION	PRIMARY OPERATING REGION	DISASTER RECOVERY REGION	RTO (HOURS)	RPO (HOURS)
United States	US-EAST-1	US-WEST-2	24	12
European Union	EU-CENTRAL-1	EU-WEST-1	24	12

The diagram below illustrates the deployment locations.

CDNS

Percipio uses advanced caching and content delivery technologies to ensure fast and reliable access to learning materials from anywhere in the world. Fastly is our primary CDN provider and ChinaCache/EdgeNext is our CDN provider in China.

A global map of Fastly POPs is accessible in the link below for reference.

https://www.fastly.com/network-map/

SECURITY OF THE CLOUD; SECURITY IN THE CLOUD

Operating a Cloud based service requires close collaboration between the hosting provider and their tenant. Skillsoft Percipio takes accountability for security in the cloud while AWS provides security of the cloud.

Additional information regarding AWS security can be found at the following URLs.

Shared Responsibility Model

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

Introduction to AWS Security

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

AWS Certification and Compliance

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

BACKUP AND RETENTION

DATABASE BACKUP AND RETENTION

Percipio backup and retention details are displayed in the following table:

AREA	RETENTION PERIOD	GRANULARITY OF BACKUPS	ADDITIONAL COMMENTS
Database	30 days	• 30 days of full backups • 7 days of point-in-time backups to within last 5 minutes	3 copies of data are always maintained in accordance with FedRAMP “3 copy mandate”. Backups transferred to remote AWS region.

LOG RETENTION

Percipio system and application log retentions are detailed in the table below:

AREA	RETENTION PERIOD
Security Logs	365 days
Other Logs	90 days

CATEGORIES OF CUSTOMER DATA STORED IN PERCIPIO

Percipio only requires supplying a unique identifier per learner by the customer in order to operate. This allows the customer to avoid storage of any PII. This is a less common configuration but is a requirement for some customers.

The table below represents the requirements and potential data types Percipio will hold as a part of service delivery for typical customers seeking the best and fully featured experience.

DATA TYPE	DESCRIPTION	OPTIONAL?
First and Last Name	PII	Yes
Email Address	PII	No
Learning Content	Channels, Courses, books, audiobooks, videos instruction, Labs	Variable

Time Spent	On Channels or Course Content	No
Collection Level Consumption	Non PII	No
Assignment Status	Non PII	No
Client Generated Content	Courseware, Additional Field as produced by Client	Yes

MAINTENANCE WINDOWS

SCHEDULED MAINTENANCE

Percipio weekly maintenance window is as follows:

13:00 to 15:00 ET Sunday

A maintenance page is erected during this interval and the site is inaccessible to customers.

This maintenance window is reserved for activities that would cause customer disruption or are inefficient if performed while the site is live. Generally, the activities performed at this time are security related.

SPECIAL MAINTENANCE

If a maintenance activity is required that exceeds the normal 2-hour duration, a special maintenance window will be announced to customers with a minimum of 30 days' notice. These are very uncommon.

COMPLIANCE REQUIREMENTS

SECURITY OVERSIGHT

Within Skillsoft, the Office of the CISO provides oversight of the security operations of the team responsible for the Percipio application.

Percipio is also subject to the audits show in the table below:

SCOPE	AUDIT	CADENCE	COMMENTS
External	FedRAMP Third Party Assessment Organization (3PAO)	Annual(Q1)	Required as part of FedRAMP
	NCC Group	Annual(Q1)	Required contractually
	UKCE+	Annual(Q2)	Mainly of interest to UK customers
	IRAP	Annual(Q4)	Mainly of interest to Australian customers
Internal	Quarterly APT	Quarterly	Conducted by the Network and Security Team

CONTINUOUS MONITORING (CONMON)

As part of the FedRAMP requirements, Skillsoft is required to maintain a Plan of Action and Milestones (POA&M) and upload vulnerability details to a government portal. This package must also be sent to the original Federal sponsor. The purpose of CONMON is to ensure that the Percipio product maintains a sufficient security posture.

VULNERABILITY MANAGEMENT TIMEFRAMES

Vulnerabilities are remediated according to criticality within the timeframes seen in the table below from the day of discovery.

SEVERITY	REMEDIATION PERIOD
Critical	Immediate
High	30 days
Medium	90 days
Low	180 days

FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FEDRAMP)

Percipio provides security in the cloud by maintaining an independently audited (annually) and validated security program. This program is based on meeting the control objectives of the FedRAMP control framework, which is based on the National Institutes of Standards & Technology (NIST) Special Publication 800-53 (SP800-53).

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The program was created to ensure that federal agencies have access to secure and reliable cloud computing services.

FedRAMP consists of a set of security controls and processes to which Percipio must adhere, to remain authorized to provide services to the United States Federal Government. The program is designed to assess the security of cloud services, such as Percipio.

A third-party assessment organization (3PAO) is selected to perform an independent assessment of Percipio's security controls. We are audited for security program capability and maturity, vulnerability assessments and penetration testing of our applications and infrastructure.

Also, Skillsoft regularly assesses our security program capability and maturity, conducts vulnerability assessments, and penetration testing of our applications and application related infrastructure.

Finally, Percipio is subject to continuous monitoring and reporting requirements to ensure that it continues to meet the FedRAMP security requirements.

Although FedRAMP is a U.S. based Regulation, Skillsoft applies this rigor to all Percipio operating environments, irrespective of country or region. Percipio achieved FedRAMP Moderate Authorization in 2022.

FedRAMP Package IDs relevant to Skillsoft's services are listed in the table below:

SERVICE	PACKAGE ID
Percipio	FR2118043605
Skillsoft Private Cloud	F1207261443
AWS US EAST/WEST	AGENCYAMAZONEW

Percipio FedRAMP Authorization to Operate (ATO) Link

https://marketplace.fedramp.gov/products/FR2118043605

CYBER ESSENTIALS

Cyber Essentials is a UK Government backed certification required by government and non-government organizations. Percipio achieved Cyber Essentials Certification for the EU deployment in 2023.

Percipio **CE Plus** certificate link:

https://registry.blockmarktech.com/certificates/bc263c2e-ea51-418a-adb2-62c422aa6e0a/

Percipio **CE** certificate link:

https://registry.blockmarktech.com/certificates/fcf780fb-de9d-4a9a-8db5-81dbf31bd59a/

IRAP

The Information Security Registered Assessors Program (IRAP) assists Australian Government customers in validating appropriate controls from the Australian Government Information Security Manual (ISM) are in place. Percipio underwent its first IRAP assessment under the September 2024 ISM.

SOC 2 – TYPE 1

Skillsoft achieved SOC2 – Type 1 compliance certification in December 2023.

SOC 2 – TYPE 2

Skillsoft achieved SOC2 – Type 2 compliance certification in April 2024.

ISO 27001

Audit completed in June 2025. Currently awaiting results.

GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that came into effect on May 25, 2018, in the European Union. The regulation aims to strengthen data protection for individuals within the EU and applies to businesses that collect, process, or store personal data of individuals in the EU, regardless of the location of the business.

The GDPR establishes several rights for individuals, including the right to access, correct, or delete their personal data, and requires businesses to obtain valid consent for data processing activities, implement appropriate security measures to protect personal data, and report data breaches to the relevant supervisory authority within 72 hours.

Failure to comply with the GDPR can result in significant fines and reputational harm for businesses. Overall, the GDPR aims to ensure that businesses handle personal data responsibly, with transparency and respect for individuals' rights.

Skillsoft is committed to complying with the privacy objectives of the GDPR, we recognize the importance of protecting personal data and respect individuals' rights to privacy. We have implemented policies and procedures for data collection, processing, and retention, and appropriate technical and organizational measures to safeguard personal data.

We strive to provide transparency and clear communication with individuals about our data practices, obtain valid consent for data processing activities, and monitor and audit data processing activities to ensure compliance with applicable laws and regulations.

In the event of a privacy incident, we are committed to responding appropriately and promptly to mitigate any harm to individuals and address the incident's root cause.

Our commitment to complying with the privacy objectives of GDPR reflects our dedication to managing and protecting personal data responsibly, ethically, and in compliance with the highest standards of data protection.

Finally, information regarding the Citizens of the European Union is kept within the European Union.

HIGH LEVEL ASSURANCE CONTROLS

Policy, Procedure, & Process

Security policies, procedures, and processes are critical components of an effective information security program. These documents provide a clear and comprehensive framework for managing and mitigating security risks and ensuring the confidentiality, integrity, and availability of sensitive information.

Keeping these documents up to date is crucial in today's rapidly evolving threat landscape. As new security threats emerge, it is essential to review and update these documents to ensure that they remain relevant and effective in addressing current and future security risks.

By having well-defined expectations, organizations can reduce the likelihood of security incidents and minimize the impact of any incidents that do occur. These documents set clear expectations for employees and other stakeholders, helping to ensure that everyone understands their roles and responsibilities in maintaining a secure and compliant environment.

ACCESS CONTROL

Our company implements access control measures to protect our critical systems and data, enabling us to restrict access only to authorized personnel and minimize the risk of unauthorized access and data breaches.

Control Functions or Areas:

- Access control policy and procedures
- Account management
- Access enforcement
- Information flow enforcement
- Separation of duties
- Least privilege
- Unsuccessful logon attempts
- System use notification

- Concurrent session control
- Session lock
- Session termination
- Permitted actions without identification or authentication
- Remote access
- Access control for mobile devices
- Use of external information systems

AWARENESS AND TRAINING

We conduct regular training and awareness programs to educate our employees on the latest security threats and best practices, empowering them to make informed decisions and minimize the risk of human error, thereby improving our overall security posture.

Control Functions or Areas:

- Security awareness and training policy and procedures
- Security awareness training
- Security awareness insider threat training
- Role-based security training
- Security training records

AUDIT AND ACCOUNTABILITY

Our company implements audit and accountability measures to keep track of all activities on our systems and data, enabling us to identify any anomalies and hold authorized users accountable for any security breaches or violations, thereby bolstering our security measures.

Control Functions or Areas:

- Audit and accountability policy and procedures
- Audit events
- Content of audit records
- Audit storage capacity
- Response to audit processing failures
- Audit review, analysis, and reporting
- Audit reduction and report generation
- Time stamps
- Protection of audit information
- Audit record retention
- Audit generation

SECURITY ASSESSMENT AND AUTHORIZATION

We ensure that our systems and data are secure our operations are compliant with relevant regulations and standards through regular security assessments, rigorous code, and infrastructure development processes and by obtaining proper authorization, mitigating the risk of security incidents and potential legal and financial penalties.

Control Functions or Areas:

- Security assessment and authorization policy and procedures
- Security assessments
- System interconnections
- Plan of action and milestones
- Security authorization
- Continuous monitoring
- Penetration testing
- Internal system connections

CONFIGURATION MANAGEMENT

Our company maintains the security and stability of our systems and data through proper configuration management, ensuring that all systems are adequately configured and managed to minimize the risk of security breaches and prevent any disruption to our operations.

Control Functions or Areas:

- Configuration management policy and procedures
- Baseline configuration
- Configuration change control
- Security impact analysis
- Access restrictions for change
- Configuration settings
- Least functionality
- Information system component inventory
- Configuration management plan
- Software usage restrictions
- User-installed software

CONTINGENCY PLANNING

We prepare for potential security incidents and other disruptions through contingency planning, developing a solid plan and response strategy to ensure business continuity even in the face of unexpected events.

Control Functions or Areas:

- Contingency planning policy and procedures
- Contingency plan
- Contingency training

- Contingency plan testing
- Alternate storage site
- Alternate processing site
- Telecommunications services
- Information system backup
- Information system recovery and reconstitution

IDENTIFICATION AND AUTHENTICATION

We prevent unauthorized access to our systems and data by implementing strict identification and authentication measures, verifying the identities of our employees and users, and ensuring that only authorized individuals can access our critical assets.

Control Functions or Areas:

- Identification and authentication policy and procedures
- Identification and authentication (organizational users)
- Device identification and authentication
- Identifier management
- Authenticator management
- Authenticator feedback
- Cryptographic module authentication
- Identification and authentication (non- organizational users)

INCIDENT RESPONSE

Our company has a quick and efficient incident response plan in place to minimize the impact of security incidents, quickly detecting, containing, and mitigating potential breaches to protect data and systems and reduce any potential damage.

Control Functions or Areas:

- Incident response policy and procedures
- Incident response training
- Incident response testing
- Incident handling
- Incident monitoring
- Incident reporting
- Incident response assistance
- Incident response plan
- Information spillage response

MAINTENANCE

Proper maintenance and updates are necessary to keep systems and data secure. By conducting regular maintenance to ensure that our systems remain up to date, it reduces the risk of security incidents and minimizes downtime.

Control Functions or Areas:

- System maintenance policy and procedures
- Controlled maintenance
- Maintenance tools
- Non local maintenance
- Maintenance personnel
- Timely maintenance

MEDIA PROTECTION

We take measures to protect our physical and digital media, which can contain sensitive data, by implementing proper media protection measures to minimize the risk of data loss or theft.

Control Functions or Areas:

- Media protection policy and procedures
- Media access
- Media marking
- Media storage
- Media transport
- Media sanitization
- Media use

PHYSICAL AND ENVIRONMENT PROTECTION

We protect our physical facilities and equipment from security threats by implementing physical and environmental protection measures to minimize the risk of theft, damage, or other security incidents.

Control Functions or Areas:

- Physical and environmental protection policy and procedures
- Physical access authorizations
- Physical access control
- Access control for transmission medium
- Access control for output devices
- Monitoring physical access
- Visitor access records
- Power equipment and cabling
- Emergency shutoff
- Emergency power
- Emergency lighting
- Fire protection
- Temperature and humidity controls

- Water damage protection
- Delivery and removal
- Alternate work site

Additionally, AWS has a very stringent regime for controlling access to their data center facilities ("the cloud"). The URL provided below provides insight into those controls.

AWS Data Center & Facility Controls

https://aws.amazon.com/compliance/data-center/controls/

PLANNING

We develop effective security strategies by conducting thorough planning and risk assessments, identifying potential threats, and developing mitigation strategies that align with our business objectives.

Control Functions or Areas:

- Security planning policy and procedures
- System security plan
- Rules of behavior
- Information security architecture

PERSONNEL SECURITY

Our employees are our first line of defense against security threats, and we ensure their trustworthiness and provide proper training by implementing personnel security measures to minimize the risk of insider threats and human error.

Control Functions or Areas:

- Personnel security policy and procedures
- Position risk designation
- Personnel screening

- Personnel termination
- Personnel transfer
- Access agreements
- Third-party personnel security
- Personnel sanctions

RISK ASSESSMENT

We identify and prioritize potential security risks by conducting regular risk assessments, focusing our resources on the most critical areas, and minimizing the risk of security incidents.

Control Functions or Areas:

- Risk assessment policy and procedures
- Security categorization
- Risk assessment
- Vulnerability scanning

SYSTEM AND SERVICES ACQUISITION

We ensure that any systems or services we acquire meet our security requirements and standards by implementing proper system and services acquisition measures, minimizing the risk of vulnerabilities and other security issues.

Control Functions or Areas:

- System and services acquisition policy and procedures
- Allocation of resources
- System development life cycle
- Acquisition process
- Information system documentation
- Security engineering principles

- External information system services
- Developer configuration management
- Developer security testing and evaluation

SYSTEM AND COMMUNICATIONS PROTECTION

We protect our systems and data from unauthorized access and other security threats by implementing rigorous system and communications protection measures, safeguarding our critical assets, and minimizing the risk of security breaches.

Control Functions or Areas:

- System and communications protection policy and procedures
- Application partitioning
- Information in shared resources
- Denial of service protection
- Resource availability
- Boundary protection
- Transmission confidentiality and integrity
- Network disconnect
- Cryptographic key establishment and management
- Cryptographic protection
- Collaborative computing devices
- Public key infrastructure certificates
- Mobile code
- Voice over internet protocol
- Secure name /address resolution service (authoritative source)
- Secure name /address resolution service (recursive or caching resolver)

- Architecture and provisioning for name/address resolution service
- Session authenticity
- Protection of information at rest
- Protection of information at rest | cryptographic protection
- Process isolation

SYSTEM AND INFORMATION INTEGRITY

We ensure the trustworthiness and reliability of our data and systems by implementing measures to maintain system and information integrity, such as data validation, data encryption, and system monitoring, to prevent unauthorized modifications, ensure data confidentiality, and minimize the risk of data loss or corruption.

Control Functions or Areas:

- System and information integrity policy and procedures
- Flaw remediation
- Malicious code protection
- Information system monitoring
- Security alerts, advisories, and directives
- Security function verification
- Software, firmware, and information integrity
- Spam protection
- Information input validation
- Error handling
- Information handling and retention
- Memory protection

AI TECHNOLOGIES

Skillsoft is committed to the responsible and ethical use if AI internally and in our products. Our corporate "Generative AI Policy" applies to all members of Skillsoft who have access to generative AI technologies, be it leveraging them or engaging third-party providers of such technologies.

Percipio uses AI technologies in the following optional product features:

PERCIPIO FEATURE	DESCRIPTION
CAISY	Simulation of conversations for coaching and training. E.g., practice confronting an employee with performance concerns.
Skilz	Skill Graph - Identify Skills related to learner Job Roles and skills related to Skillsoft stock content, linked content and custom content.
QNA	Percipio Search - AI-enabled search bar on the Percipio main page. Course Q&A – AI enabled Q&A tab on course player.
Curator Palette	Tool to allow customer admins to search for materials to build customer originated curated content.

Skillsoft utilizes Microsoft AI Services in the Azure Commercial Cloud within the same geography as their Percipio deployment. Customers deployed in the US will use US Azure Infrastructure while customers deployed in the EU will use EU Azure Infrastructure.

Communication between Percipio and the AI services in Azure is by way of APIs over TLS 1.2.

"Prompt moderation exception" is in place, ensuring no AI model inputs or outputs are logged or reviewed by Microsoft. Additionally, organizations and learners can opt-out of having conversation inputs logged.

FINAL STATEMENT

We hope that this document has provided you with valuable insights into the security measures that we have in place to protect your data and ensure the availability and integrity of our systems.

Reach out to your Skillsoft contact and ask to speak to our Network, Security, and Infrastructure group if you have any questions or concerns.

APPENDIX A – SECURITY CHECKLIST

The checklist below is intended to provide a quick reference for status of commonly requested security measures:

CATEGORY	FEATURE	✓/✗
Assessments	IRAP Protected Level (September 2024 ISM)	✓
Audits	Internal Audit	✓
	3rd Party Audits (Annual)	✓
Antivirus	Next-generation non-signature-based antivirus protection	✓
Backup	Multiple copies (3 copy mandate)	✓
	Offsite Backup Storage	✓
	Encrypted backups	✓
Bug Bounty	Formal Bug Bounty Program	✓
Business Continuity	Corporate Business Continuity Plan Tested Annually	✓
Certifications (Skillsoft)	FedRAMP Moderate Rev 5	✓

	UKCE/UKCE+	✓
	SOC2 – Type 1	✓
	SOC2 – Type 2	✓
	TX-RAMP (Level 2 Certification)	✓
	ISO 27001	In Progress
Certifications (Public Cloud Providers)	ISO 27001	✓
	SOC2 – Type 2	✓
Development Tools	Static Code Analysis	✓
	Open-Source Licensing	✓
Disaster Recovery	Product Specific Disaster Recovery Plan Tested Annually	✓
Encryption at Rest	Database Storage	✓
	Object Storage	✓
	File Storage	✓
	Block Storage	✓

Encryption In Transit - External	Between Learner and Percipio Application	✓
Encryption In Transit - Internal	Between Percipio Microservices within the Percipio Application	✓
Geo-blocking	In place for embargoed countries	✓
Insurance	Cyber Liability Insurance	✓
Mail	Domain-based Message Authentication, Reporting and Conformance (DMARC) compliant mail	✓
	DomainKeys Identified Mail (DKIM)	✓
Phishing Attack Simulator	Phishing Attack Simulator used to test and educate employees	✓
Risk Management Framework	FedRAMP/NIST 800-53 Rev 5	✓
Security - General	Distributed Denial of Service System (DDoS)	✓
	Intrusion Prevention System (IPS)	✓
	Web Application Firewall (WAF)	✓
	Data Loss Prevention (DLP)	✓
	Outbound Whitelisting	✓

	Privileged Access Management (PAM)	✓
	Security Information and Event Management (SIEM)	✓
	Ransomware Protection	✓
	OSCP Stapling (TLS Certificate Status Request Extension)	✓
Staff - General	Background Checks	✓
Staff – Relevant Policy	Rules of Behavior	✓
	Code of Business Conduct and Ethics	✓
Staff - Dedicated Roles	Chief Information Security Officer (CISO)	✓
	Data Protection Officer (DPO)	✓
	Internal Audit	✓
Threat Intelligence	Industry Leading Threat Intelligence Platform Subscription	✓
Threat Modeling	STRIDE Framework	✓
Training	Yearly Security Awareness Training Requirement	✓

	Anti-Counterfeit Training Requirement	✓
Vulnerability Management Tooling	Container Scanning	✓
	Operating System Scanning	✓
	Compliance Scanning (CIS)	✓
	Automated Penetration Testing	✓
	Manual Penetration Testing	✓

APPENDIX B - PRODUCT DOCUMENTATION FOR ROLE BASED ACCESS CONTROL (RBAC)

The link below to Percipio product documentation is a wealth of information but one section will be of particular interest to customers in security roles – "Percipio for Administrators".

The Percipio application has the concept of administrators, users, roles and privileges which allows the customer to securely manage their own Percipio site. See the link below for details:

https://documentation.skillsoft.com/en_us/percipio/Content/home.htm

APPENDIX C - PLATFORM WHITELIST/SAFELIST REQUIREMENTS

The Percipio platform whitelist/safelist requirements are commonly requested, and direct link is provided below for your convenience.

https://documentation.skillsoft.com/en_us/percipio/Content/A_Administrator/percipio_sys_reqs_platform_safelist.htm

APPENDIX D - PRIVACY NOTICE LINK

Follow the link below to the Skillsoft Privacy Notice:

https://www.skillsoft.com/about/privacy-notice