# Services des opérations cloud (CO) de Skillsoft
# Percipio hébergé dans l'UE

## Historique des révisions

| Date | Version | Description | Auteur |
|---|---|---|---|
| 27-03-2019 | 1.0 | Description des opérations cloud et du cloud privé dans l'UE | Opérations cloud |

## Introduction

Skillsoft propose Percipio selon le modèle logiciel en tant que service (SaaS). Les utilisateurs accèdent au logiciel Percipio via le web : cela permet de simplifier la gestion de l'application web devant être accessible via l'internet dans le monde entier, 24h/24, 7j/7 et 365 jours par an.

Grâce au modèle SaaS, le service informatique de nos clients n'ont plus besoin de s'inquiéter des éléments suivants :

- Coûts matériels
- Coûts de licences logicielles
- Contrôle de l'application
- Formation d'experts internes pour l'assistance liée à la solution de formation en ligne
- Gestion des mises à niveau de l'application et du contenu
- Allocation de personnel informatique aux opérations de maintenance récurrentes
- Gestion de la sécurité pour l'application
- Gestion des sauvegardes/restaurations
- Augmentation du personnel d'assistance

Le service des opérations cloud (CO) de Skillsoft a développé des stratégies et des processus pour garantir les performances de l'application tout en conservant des normes de sécurité élevées. Ci-dessous vous trouverez une description de ces processus et des services CO globaux que fournit Skillsoft. Pour les entreprises limitant les adresses IP accessibles dans l'entreprise, Skillsoft fournit une plage d'adresses IP qui doivent être ouvertes pour que l'application Percipio fonctionne correctement. Si vous souhaitez plus d'informations sur les plages d'adresses IP, l'équipe responsable du compte client pourra vous en fournir.

## Bouclier de protection des données / RGPD

Skillsoft s'engage à protéger vos données et respecte le règlement européen sur la protection des données tel qu'il est inscrit dans les lois applicables d'un État membre, comme le Data Protection Act de 1998 au Royaume-Uni. Skillsoft a mis en place des mesures et processus de protection des données pour garantir la conformité avec le règlement général sur la protection des données (RGPD).

Skillsoft a déployé un outil de TrustArc pour dresser l'inventaire de toutes les applications stockant les données personnelles des utilisateurs européens. Skillsoft a également déployé des outils permettant aux clients d'exercer leur droit à l'oubli.

Cette année, Skillsoft poursuit le processus de certification du Bouclier de protection des données (Privacy Shield). Nous avons engagé un cabinet de conseil externe, spécialisé en confidentialité des données. Ce cabinet réalise une évaluation complète des processus commerciaux de Skillsoft, des pratiques en matière de collecte et d'utilisation des données personnelles européennes et des flux de données personnelles de l'UE aux États-Unis afin d'évaluer nos stratégies et pratiques de protection des données personnelles par rapport aux exigences du bouclier de protection des données. Une fois ce processus terminé et toutes les modifications nécessaires apportées aux stratégies et procédures, Skillsoft va se lancer dans l'autocertification Bouclier de protection des données auprès du ministère américain du commerce.

Nous nous engageons à terminer ce processus d'évaluation et d'autocertification dès que cela sera raisonnablement possible pour que nous puissions utiliser le bouclier de protection des données comme mécanisme de transfert afin de respecter les exigences européennes en matière de protection des données. D'ici là, Skillsoft respectera les clauses contractuelles standard qui gouvernent ces transferts. L'accord de clause type est disponible pour les clients européens de Skillsoft s'ils le souhaitent.

## Description de l'application Percipio

Percipio est une application web développée sur une architecture microservice. L'application utilise la plateforme OpenShift de RedHat, les conteneurs Docker, Kubernetes, Kafka, les bases de données PostgreSQ L et les bases de données Cassandra pour les analyses et rapports. Elle utilise d'autres technologies qui sont les meilleures de l'architecture microservice. L'application Percipio repose également sur Java et Ruby. Elle utilise la base de données SQL pour stocker différents paramètres de configuration ainsi que les informations d'identification et les enregistrements de progression des apprenants. Les clients sont contenus séparément dans la base de données SQL sous un identifiant d'organisation unique à chaque organisation.

L'application Percipio utilise une architecture mutualisée avec des identifiants uniques. Tous les clients utilisent la même base de données et le même schéma, mais les lignes de la table ont un identifiant d'organisation unique utilisé lors de l'extraction des données pour une organisation. Dans une même organisation, un identifiant utilisateur unique est utilisé, dans certains cas, pour filtrer davantage les données à celles d'un utilisateur unique.

Les identifiants uniques sont générés avec le format v4 UUID (https://en.wikipedia.org/wiki/Universally_unique_identifier). Ils sont également générés de manière aléatoire par des bibliothèques logicielles conformes à RFC4122 (https://tools.ietf.org/html/rfc4122#section-4.1.3i ). Il y a très peu de chances que ces identifiants puissent être devinés (https://stackoverflow.com/questions/4878359/what-is-the-probability-of-guessing-matching-a-guid).

### Données personnelles et autres données d'utilisateur

L'application stocke dans sa base de données SQL les données d'utilisateur suivantes :

- prénom,
- nom,
- adresse e-mail,
- activité, comme l'accès aux cours, livres et livres audio,
- temps passé sur les pages Canal et Cours,
- utilisation au niveau des collections et
- statut du parcours.

Les utilisateurs-apprenants peuvent accéder à l'application via un navigateur web sur le port 443. Les cours sont lancés via la JWPlayer HTML5.

### Équilibrage de charge

Tous les produits de la génération actuelle sont extrêmement évolutifs et disponibles grâce à une architecture d'équilibrage de charge matérielle classique. Tous les composants temps réel de l'application comportent des options d'évolutivité horizontale et verticale. Ils font également l'objet d'un suivi constant par rapport aux critères de performance clés et évoluent selon les besoins à la demande. Les composants de l'infrastructure centrale sont implémentés selon un modèle de basculement actif-actif ou actif-passif.

### Services de centre de données et de colocalisation

Skillsoft a contracté des services de centre de données et de colocalisation auprès de British Telecom (BT), fournisseur de services de niveau 3 et plus. Le centre de données se trouve à Francfort en Allemagne. Les centres de données BT fournissent une connectivité de large bande passante redondante et une évolutivité qui permettent à Skillsoft de développer son service d'hébergement rapidement et efficacement. L'accès sécurisé comprend plusieurs niveaux de contrôles d'accès, physiques et numériques. BT propose une connectivité réseau hautement fiable et des installations de colocalisation de pointe pour créer le meilleur environnement d'exploitation possible pour Skillsoft et ses clients.

Le centre de données BT est équipé d'un système de détection des incendies VESDA et d'un système d'extinction des incendies FM-200. Une alimentation redondante 2N fournit les alimentations doubles et les batteries de sauvegarde, les systèmes de refroidissement et les générateurs.  Un système de régulation de la climatisation

redondant N+1 alimente les systèmes de refroidissement principal et de secours, les tours de refroidissement et le stockage d'eau. Un centre d'opérations réseau (NOC) local surveille les opérations du centre de données en continu. BT a obtenu un indicateur d'efficacité énergétique de 1,3. L'accès physique au centre de données BT est sécurisé par des gardes 24h/24et 7j/7, un réseau de télésurveillance en circuit fermé (intérieur et extérieur), un accès électronique à toutes les entrées du centre de données, y compris des systèmes de gestion des clés électroniques et des armoires et cages à clé individuelle. Le site est entouré d'une clôture périphérique dont le portail d'entrée est contrôlé et surveillé à distance par le personnel de sécurité de BT grâce à la télésurveillance.

Les centres de données BT ont reçu les certifications suivantes :

ISO 9001 : gestion de la qualité

ISO 20000 : processus informatique, ITIL

ISO 27001 : gestion de la sécurité

ISO 14001 : management environnemental

Vous pouvez obtenir de plus amples informations sur les centres de données et les services de colocalisation BT directement auprès de BT.

## Contrôle des appareils réseau

### Description du réseau, des routeurs, des commutateurs et des pare-feu

Consciente du caractère critique des infrastructures réseau et de sécurité, Skillsoft a investi dans les meilleurs appareils de fournisseurs comme Cisco et F5 Networks. Ces investissements stratégiques soulignent notre volonté de toujours fournir des services exceptionnels.  Les infrastructures réseau sont conçues pour être évolutives et résister aux pannes conformément aux nombreux conseils sur lesquels se basent les fournisseurs de services internet.

Un système de prévention et de détection des intrusions et de pare-feu se charge de la sécurité du périmètre.  Ce système multicouche et multifournisseur apporte aux clients le meilleur niveau de protection possible face aux attaques de service et tentatives d'intrusion. Il donne également à Skillsoft la flexibilité nécessaire pour répondre aux nouvelles menaces.

Tous les systèmes sont élaborés à partir d'images prérenforcées et normalisées, basées sur les meilleures pratiques du secteur. Les images système sont régulièrement examinées pour garantir leur réactivité face à des technologies et des menaces en constante évolution.

Enfin, Skillsoft fait faire un audit de sécurité annuel de son environnement CO par un tiers. Aucune des évaluations réalisées n'a révélé de vulnérabilité de risque élevé dans les systèmes de Skillsoft.

## Gestion des programmes de contrôle

### Procédures de récupération et de redémarrage

Pour que le personnel CO de Skillsoft soit alerté dès que possible de toute condition pouvant affecter les services, une infrastructure de surveillance complète a été mise en place. Des gouvernances clairement définies informent l'ingénieur CO assigné des actions autorisées sans besoin d'escalade et donnent des détails spécifiques quant à la réalisation des mesures prescrites. Si une condition apparaît pour laquelle il n'y a aucune procédure définie, le problème doit être notifié immédiatement au responsable hiérarchique.

### Restrictions d'accès système

Seul le personnel CO a un accès privilégié à tous les systèmes de cloud privé afin de respecter la confidentialité des données que nos clients confient à Skillsoft et afin de fournir un environnement CO le plus stable possible. En aucun cas l'accès système n'est accordé à une tierce partie extérieure à CO, à l'exception des fournisseurs de service sous contrat avec Skillsoft pour services professionnels ou d'assistance directe. Aucun fournisseur de service tiers n'a accès aux données des clients.

### Documentation système

Une documentation exhaustive a été rédigée et couvre tous les aspects de la construction du système, de l'installation des application et de la configuration et gestion des produits. Ces documents sont mis à jour en permanence afin d'y consigner les stratégies et procédures les plus récentes. Toutes les versions des documents sont contrôlées rigoureusement et toute modification est soumise à la révision et à l'approbation des parties concernées.

### Protection contre les accès non autorisés

L'accès privilégié à toute l'entité CO de Skillsoft est strictement contrôlé et disponible uniquement au personnel CO. L'accès n'est accordé à aucun autre personnel que l'équipe CO et cela concerne tous les systèmes. Des protocoles strictes et appliqués systématiquement garantissent que tous les accès sont suspendus immédiatement après toute tâche affectant le personnel CO.

## Procédures de protection de données

### Stratégie globale de sauvegarde

Les sauvegardes système ne sont pas prévues aux fins suivantes :

- Archivage de données
- Protection contre les scénarios qui ne sont pas directement liés à une perte de données

La sauvegarde des données est effectuée avec CommVault Simpana et comprend deux phases :

- Sauvegarde de disques : utilisation de la baie de stockage sur disques pour stocker les sauvegardes sur le site d'hébergement, ce qui les rend disponibles pour toute restauration rapide si nécessaire. Les sauvegardes seront les sauvegardes de données récentes.
- Sauvegarde sur bande : utilisation des supports LTO6 de sauvegarde. Les bandes sont chiffrées à l'aide d'une méthode de chiffrement logicielle conforme à la norme FIPS 140-2 dans la plateforme même. Cela permet d'avoir une phrase secrète AES de 256 bits devant contenir au moins 16 caractères. Skillsoft utilisera une chaîne de 64 caractères générée de manière aléatoire.

### Calendrier des sauvegardes

La sauvegarde des systèmes sera effectuée selon le calendrier ci-dessous :

| Classe d'informations | Fréquence/type | Conservation sur disque | Conservation hors site | Commentaire |
|---|---|---|---|---|
| Bases de données relationnelles Percipio | Quotidienne | 90 jours | s.o. | **Principalement données d'application client** |
| | Hebdomadaire | 90 jours | 90 jours | |
| Stockage réseau | Quotidienne | 90 jours | s.o. | **Inclut les jeux de données d'application, de référentiels et administratifs** |
| | Hebdomadaire | 90 jours | 90 jours | |

| | | | | |
|---|---|---|---|---|
| | | | | |

## Retrait des supports de sauvegarde

Le support sera retiré et éliminé tel qu'il est décrit dans la politique de destruction des actifs numériques de Skillsoft.

Avant le retrait et l'élimination, le service des opérations cloud (CO) doit s'assurer que :

- Le support ne contient plus d'images de sauvegarde actives.
- L'ancien contenu ou le contenu actuel du support ne peut pas être lu ou récupéré par une partie non autorisée.

## Vérification des sauvegardes

Au quotidien, les informations consignées générées à partir de chaque tâche de sauvegarde sont examinées par l'administrateur de sauvegarde aux fins suivantes :

- Rechercher et corriger les erreurs.
- Surveiller la durée de la tâche de sauvegarde.
- Optimiser les performances de sauvegarde, le cas échéant.
- Le service informatique identifiera les problèmes et prendra les mesures correctrices nécessaires pour réduire les risques associés aux sauvegardes ayant échoué.
- Des restaurations tests aléatoires seront effectuées une fois par semaine pour vérifier la réussite des sauvegardes.

L'hébergement conservera des enregistrements illustrant la révision des journaux et les restaurations tests pour démontrer la conformité de cette stratégie à des fins d'audit.

## Récupération des données

En cas de panne catastrophique du système, les données sauvegardées hors site seront mises à disposition des utilisateurs dans un délai de 3 jours ouvrables si l'équipement détruit a été remplacé entre-temps.

En cas de panne non catastrophique du système ou d'une erreur d'utilisateur, les données sauvegardées sur site seront mises à disposition des utilisateurs dans un délai d'un 1 jour ouvrable.

### Demandes de restauration

En cas de suppression ou d'altération accidentelle des informations, les demandes de restauration doivent effectuées via le support technique de Skillsoft. Le support technique de Skillsoft ouvrira alors un ticket attribuant la demande de restauration à l'équipe Opérations cloud globales - Support technique pour l'hébergement.

## Gestion des incidents

Tous les systèmes de cloud privé sont globalement surveillés pour leur disponibilité depuis plusieurs emplacements physiques. Des alertes visuelles et sonores sont générées 1 minute après une défaillance de service et des alertes par e-mail sont générées 2 minutes après. Une action immédiate est prise pour restaurer les services altérés. Tous les événements affectant les services sont consignés et analysés à la fois par l'équipe d'ingénierie logicielle et par l'équipe CO pour s'assurer que l'événement est bien compris et que des mesures sont prises pour atténuer toute exposition future à l'événement.

### Performance lente des applications

En plus de faire le suivi de la disponibilité des services de cloud privé, des mesures complètes sont mises en place pour protéger contre la latence temporaire ou mineure des applications. Une infrastructure de surveillance redondante et dispersée géographiquement fournit des notifications visuelles, sonores et par e-mail pour tous les événements de surveillance dépassant le délai autorisé. Les moniteurs transactionnels simulent l'activité de l'utilisateur pour donner un indicateur fiable des performances générales du système, de la perspective de l'utilisateur final.

### Gestion des brèches de sécurité

En cas de compromission des systèmes ou services de cloud privé, l'équipe CO de Skillsoft mettra immédiatement en place un verrouillage de l'environnement pour bloquer toutes les communications entrantes et sortantes de l'environnement du centre de données. Une connexion distante privilégiée sera maintenue pour l'équipe réseau et sécurité CO afin de garantir une résolution du problème la plus rapide possible. Tous les efforts possibles doivent être fournis pour clore la brèche, stabiliser de nouveau les systèmes et limiter l'exposition des données client. Une analyse détaillée des événements doit être effectuée le plus vite possible et partagée avec nos clients, le cas échéant.

### Processus de communication avec les clients

Ce sont l'équipe de support technique et les consultants en apprentissage de Skillsoft qui communiquent avec le client. Des analyses des causes d'origine sont disponibles si le client le demande.

## Récupération des systèmes après un événement affectant les services

### Défaillance matérielle

De nombreux systèmes de l'environnement de cloud privé ont une charge matérielle équilibrée et la perte d'un système n'affecte pas les services. Lorsqu'une redondance matérielle n'est pas fournie, des systèmes de secours entièrement configurés sont disponibles pour une utilisation immédiate. Les stratégies et procédures de récupération sont documentées pour permettre une réponse rapide à ces incidents et à restaurer les services de manière rapide et efficace.

### Défaillance d'application

Les défaillances d'application sont détectées grâce à une surveillance continue des systèmes et le délai de résolution est inférieur à 10 minutes. Les procédures de correction sont documentées et toutes les défaillances d'application sont envoyés à l'équipe d'ingénierie logicielle pour examen.

### Perte de réseau

Une infrastructure réseau entièrement redondante permet à Skillsoft de fournir une infrastructure hautement disponible. La redondance est intégrée à tous les niveaux, y compris au niveau de la connexion internet. Des tests de basculement sont effectués régulièrement pour garantir que les modifications de configuration et l'installation de correctifs n'affectent pas la fiabilité de la tolérance de pannes.

### Performances d'application altérées (c.-à-d. latence)

La latence des applications est détectée grâce à une surveillance continue des systèmes et le délai de résolution est inférieur à 10 minutes. Les procédures de correction sont documentées et tous les événements de latence d'application sont envoyés à l'équipe d'ingénierie logicielle pour examen.

### Récupération sécurisée

Dans l'éventualité peu probable qu'une personne tierce doive être impliquée dans la récupération d'un système, cette implication fera l'objet de conditions contractuelles officielles, examinées et précisées par le service juridique de Skillsoft avant le début de l'implication. Les parties tierces travaillant directement avec des informations sensibles sont soumises à et liées par des accords de confidentialité.

### Récupération d'urgence

Pour faciliter une récupération rapide, l'équipe des services des opérations cloud de Skillsoft a élaboré un plan de récupération d'urgence détaillant les parties responsables, le protocole de communication et les étapes à effectuer en cas de sinistre. Skillsoft possède un site d'hébergement redondant situé à Northborough, dans le Massachusetts aux États-Unis. Le centre de données de récupération d'urgence est géré par Iron Mountain. Le site redondant se

trouve à plus de 8 000 km du site d'hébergement principal situé à Francfort en Allemagne. En cas de sinistre, les clients auront l'option de redéployer les produits SaaS de Skillsoft aux États-Unis. Les sites des clients seront redéployés après obtention de l'accord écrit des clients. Skillsoft développe actuellement un plan de récupération d'urgence qui conservera les données dans l'UE. L'objectif est que ce plan soit prêt pour la fin de l'année 2019.

### Conformité à l'architecture standard

Tous les systèmes de production sont déployés conformément aux meilleures pratiques de sécurité. Tous les systèmes sont en fait des répliques d'une image principale. Le processus de déploiement est ainsi efficace et le délai de récupération après une défaillance de système irrécupérable s'en trouve réduit.

Les mises à jour OEM les plus récentes sont chargées sur tous les systèmes d'exploitation. Ces opérations sont effectuées à l'aide d'outils développés en interne et en externe.

Pour limiter les accès aux comptes d'administrateur ou super-utilisateur non autorisés, tous les systèmes sont renforcés selon les meilleures pratiques du secteur et des fournisseurs :

- Normes d'appellation et de mot de passe complexes
- Paramètres du contrôle d'accès utilisateur
- Redirection vers des comptes désactivés.

Tous les systèmes sont vérifiés pour garantir que les services inutiles ou potentiellement exploitables sont configurés pour être désactivés à la mise sous tension.

### Gestion des modifications – Rôles et responsabilités

Les responsables technologiques ont un cadre défini d'approbations et agissent en tant qu'autorité d'approbation pour les réglages relevant de leur domaine de compétence. Les modifications ayant un impact plus large sont envoyées pour examen avec les parties prenantes concernées. Les parties prenantes examinant les demandes de modification sont les suivantes :

- Responsable réseau et sécurité
- Responsable des services d'application
- Responsable des bases de données
- Responsable SANS et stockage
- Directeur des opérations cloud
- VP principal des opérations cloud globales

Le directeur des opérations cloud et le VP principal des opérations cloud globales possèdent un droit de véto final sur toutes les demandes de modification.

### Gestion des configurations du système

Les réglages effectués sur les images système ou les configurations font l'objet d'un contrôle strict via un processus d'examen et d'approbation à plusieurs impliquant des personnes des équipes de direction, réseau et sécurité, des analystes de système et des ingénieurs de système. La documentation est mise à jour immédiatement pour refléter la reconfiguration du système.

### Processus de modification, test et processus d'approbation

Les demandes de modification sont envoyées par la partie initiatrice au responsable technologique concerné pour étude préliminaire. Le responsable en charge demandera alors des conseils au directeur CO afin de déterminer l'étendue de la modification et d'établir un cycle d'approbation. Lorsque possible, les modifications sont vérifiées via une implémentation préliminaire dans un environnement de préproduction. Dans certains cas, elles requièrent et reçoivent un test de charge effectué par une équipe d'automatisation dédiée.

Pour garantir la qualité du travail, les modifications apportées à l'environnement sont vérifiées de manière continue par des superviseurs CO. Les architectes CO réalisent des audits physiques tous les trimestres pour confirmer que l'environnement répond aux normes définies.

### Spécifications de configuration et de sécurité

Skillsoft applique une stratégie très restrictive par rapport aux contrôles d'accès et aux stratégies pour les appareils réseau. Les règles des systèmes de détection et de prévention des intrusions et des pare-feu sont examinées et contrôlées en continu à la recherche d'événements suspects. La configuration des appareils est normalisée et bien documentée. Les réglages apportés aux configurations et stratégies sont reflétés dans la documentation associée au système ou à l'appareil.

### Contrôle de la configuration

Si un ingénieur réseau modifie les réglages d'un appareil, ces modifications requièrent l'approbation du responsable réseau. Dans certains cas, il faudra également l'approbation du directeur CO. Tout réglage d'un aspect de la configuration système hôte requiert l'examen et l'approbation de l'architecte de système principal et, dans certains cas, du directeur CO. Les réglages ou modifications apportés à la configuration sont reflétés dans la documentation associée au système ou à l'appareil.

## Gestion des mots de passe, des comptes et de la sécurité

### Gestion des mots de passe

L'utilisation de noms d'utilisateur et de mots de passe génériques est interdite. Les administrateurs reçoivent des informations de connexion individuelles et peuvent gérer leurs propres mots de passe selon la stratégie de mots de passe appliquée au domaine.

### Expiration des mots de passe

Les mots de passe de compte d'utilisateur expirent tous les 30 jours. Ils doivent remplir des conventions de complexité strictes et ne peuvent pas être réutilisés. L'expiration des mots de passe est appliqué via des objets de stratégie de groupe (GPO).

### Longueur et complexité des mots de passe

Les mots de passe doivent répondre à des exigences de complexité, y compris une restriction de nombre minimal de caractères, et à des exigences de caractères non alphanumériques et de casse mixte. Ce sont les objets de stratégie de groupe (GPO) qui gèrent la longueur et la complexité des mots de passe.

### Protection des mots de passe

Des efforts sont faits pour limiter la communication des mots de passe aux canaux verbaux. Les mots de passe sont fournis selon le principe d'accès sélectif (« need-to-know basis »). Lorsqu'il n'est pas possible de communiquer les mots de passe verbalement, les combinaisons de nom d'utilisateur et de mot de passe sont communiqués séparément et seulement aux personnes concernées. Le partage des mots de passe de compte d'utilisateur est strictement interdit.

### Description de la sécurité physique

Tous les systèmes de cloud privé de Skillsoft se trouvent sur un site tiers conforme à l'ISO 27001 et fournissant un contrôle d'accès 24h/24 et 7j/7 selon un calendrier de contrôle d'accès défini. Le site utilise des gouvernances de contrôle d'accès à plusieurs couches, notamment des sas de sécurité, une télésurveillance, un accès par carte uniquement et des gardes 24h/24 et 7j/7. Les sites ne sont pas identifiables.

### Environnement – Description de la sécurité

Une infrastructure de défense de périmètre multicouche garantit la meilleure protection possible contre les accès non autorisés ou les activités malveillantes. Les mesures incluent une stratégie de pare-feu très restrictive, des

systèmes de prévention et de détection des intrusions avec critères spéciaux et réseau ainsi qu'une infrastructure antivirus complète et à jour.

### Systèmes – Description de la sécurité

Tous les systèmes sont construits à partir d'images prérenforcées et normalisées selon les meilleures pratiques du secteur et conformément aux configurations logicielle et système spécifiques de Skillsoft. La gestion des correctifs de routine est contrôlée par un logiciel de gestion des correctifs centralisée pour garantir une posture cohérente et à jour.

### Personnel –– Gestion de la sécurité

Les actions liées aux employés (recrutement, licenciement, suspension, etc.) sont coordonnées entre les ressources humaines et le service informatique pour répondre immédiatement aux changements de statut de tout le personnel CO. De plus, la direction CO sera avisée de tous les départs d'employé Skillsoft au cas où des mesures spéciales doivent être prises pour se protéger contre les actions d'anciens employés ayant des connaissances ou une compréhension exclusives des logiciels propriétaires de Skillsoft.

### Chiffrement des appareils mobiles et ordinateurs portables des employés

Skillsoft utilise un logiciel d'exploitation des stratégies de chiffrement au niveau fichier qui chiffre de manière homogène les fichiers statiques et en transit selon les niveaux de risques, tel qu'il est défini dans la politique d'informations. Le facteur de risque est déterminé selon le contenu, le contexte et le type de données. Toutes les données client sont considérées comme des informations sensibles et traitées comme telles. Pour les données qui peuvent être potentiellement copiées sur des périphériques auxiliaires tels que des clés USB, des CD ou des DVD, le service informatique a déployé un logiciel de protection des informations d'entreprise qui va détecter et empêcher les employés de Skillsoft de transférer des informations clients sensibles vers des dispositifs mobiles (c.-à-d. CD-RW/DVD-RW, clés USB, disques durs, ordinateurs de poche, appareils photo, téléphones portables).

### Accès à l'environnement de cloud privé

L'accès et les communications vers l'environnement de cloud privé sont sécurisés avec un chiffrement client ou de site à site. Les tunnels de site à site fournissent un accès au service ou au port et sont limités aux sous-réseaux réservés au cloud privé de Skillsoft. Une authentification des accès à distance est intégrée étroitement à la sécurité du domaine existante et fournit un point d'administration central. L'accès à distance est limité au personnel CO. Cette stratégie est universelle et exhaustive, car elle inclut l'administration, les sauvegardes, etc. En aucun cas les développeurs logiciels, les spécialistes en formation, les ingénieurs en application, le service informatique d'entreprise ou les responsables de compte ne se voient accorder un accès privilégié.

## Accès distant à l'environnement de cloud privé

Seuls les ingénieurs CO ont accès aux systèmes de cloud privé. L'accès aux divers sous-systèmes est divisé selon les rôles et les responsabilités. Chaque ingénieur a un ID d'utilisateur et un mot de passe uniques et gérés via une liste de contrôle d'accès donnant l'accès uniquement aux systèmes qui relèvent de la responsabilité de l'ingénieur. Comme la plupart des ingénieurs CO requièrent un accès à l'environnement de cloud privé 24h/24 et 7j/7, ils ont des ordinateurs portables. Ces derniers ne comportent que le système d'exploitation et un logiciel de VPN. Pour accéder à l'environnement de cloud privé, les ingénieurs CO se connectent à distance de leur ordinateur portable à leur ordinateur de bureau situé sur le site Skillsoft qui comporte le logiciel VPN qui fournit la connectivité à l'environnement de cloud privé. L'accès est authentifié via une authentification à deux facteurs de RSA Security. Les mots de passe d'application sont modifiés tous les 30 jours ou lorsqu'un employé CO quitte son poste.

## Test de pénétration annuel tiers

Dans un effort continu d'amélioration de la sécurité de l'environnement de cloud privé, Skillsoft conclut des contrats avec des organisations de sécurité tierces pour qu'elles effectuent une évaluation annuelle et exhaustive des vulnérabilités et des tests de pénétration pour l'environnement de cloud privé. Ces évaluations examinent les stratégies de pare-feu, les stratégies de détection et de prévention des intrusions, les niveaux de correctif système et les vulnérabilités face aux exploitations logicielles et attaques par force brute connues. Les résultats de l'évaluation sont transmises aux clients sur demande.

## Divulgation des plateformes, technologies et fournisseurs

Pour contrer la collecte de renseignements, Skillsoft ne divulguera à aucun client, sous quelque condition que ce soit, la marque, le modèle ou le fabricant de tout appareil réseau ou de sécurité utilisé dans l'environnement de cloud privé. Cela inclut la divulgation d'informations relatives aux éléments suivants :

- Paramètres/logiciels/matériels associés au pare-feu
- Paramètres/logiciels/matériels aux systèmes de détection des intrusions
- Test de pénétration réseau
- Analyse des vulnérabilités
- Topologie réseau
- Schéma IP interne
- Paramètres de configuration et de sécurité des systèmes d'exploitation
- Éditeurs et version des logiciels utilisés

### Maintenance système planifiée

Description du calendrier de la maintenance système planifiée

Les opérations de fenêtre de maintenance de routine (lorsque ces dernières affectent les services) sont limitées à deux heures par semaine.  Les fenêtres de maintenance spéciale demandant plus longtemps peuvent être demandées de temps à autre. Un préavis de 14 jours sera donné pour ces maintenances spéciales.

Les activités réalisées lors de ces fenêtres de maintenance peuvent inclure, sans s'y limiter, l'entretien et le remplacement du matériel, les mises à jour correctives du système, les améliorations d'infrastructure et les nouvelles versions des logiciels Skillsoft.

### Maintenance d'urgence

Skillsoft se réserve le droit d'effectuer des activités de maintenance non planifiées lorsque retarder la maintenance en question peut poser des risques importants à la disponibilité et/ou à la sécurité des services fournis.  Tout est fait pour coordonner à l'avance ces activités de maintenance imprévues avec les clients et de les effectuer à un moment où cela a le moins d'impact possible dès que les conditions s'y prêtent.

### Calendrier de maintenance

Toutes les activités de maintenance planifiées sont coordonnées et programmées à l'avance dans des fenêtres ayant des limites définies.  Toutes les activités font l'objet d'un examen critique pour garantir le timing et que les activités ne se chevauchent pas.

### Gestion de la sécurité

Seul le personnel CO peut réaliser les activités de maintenance et l'accès est contrôlé strictement par des mesures de sécurité impliquant plusieurs parties.

### Sans fil au bureau

Skillsoft fournit à ses employés un accès sans fil sur les sites Skillsoft. Le service sans fil utilise le chiffrement WPA2 Enterprise pour accéder aux environnements réseau de Skillsoft. L'accès sans fil requiert une authentification unique. Les journaux d'accès sont enregistrés dans un un emplacement central et sont passés en revue pour des tentatives d'accès échouées. Une détection des réseaux sans fil non autorisés est effectuée en continu pour empêcher toute activité malveillante.

Les points d'accès sont configurés pour utiliser l'authentification RADIUS. Un SSID sécurisé unique est configuré. Le trafic sans fil est sécurisé et géré avec des stratégies de pare-feu. Les ports autorisés sont limités aux ports HTTP (80), HTTPS (443) et VPN (TCP/UDP).

L’accès sans fil est distinct avec sa propre interface Ethernet sur le pare-feu de Skillsoft et n’a pas accès aux ressources d’entreprise internes. Pour accéder aux ressources d’entreprise, il faut utiliser le VPN.

## Code production – Contrôle des modifications

### Développement produit

Le développement logiciel lié aux produits est effectué par les ingénieurs logiciels de Skillsoft comprenant les Scrum Masters, les responsables DevOps, les architectes de squad, les ingénieurs logiciels et les développeurs de bases de données. Le service d’ingénierie logicielle est divisé en équipes selon les différents domaines d’expertise requis par les divers produits et leur cycle de vie de développement logiciel respectif.

### Processus d’assurance qualité

Une équipe d’assurance qualité dédiée garantit que tous les logiciels mis à disposition des clients sont de la meilleure qualité possible et ont d’excellentes performances.  Cette équipe a un droit de véto final sur tous les ensembles logiciels allant sur les systèmes de production.

### Processus de qualification

Une matrice de test exhaustive et approfondie est appliquée à la fonctionnalité de test des sprints Percipio et à leur prise en charge de toutes les technologies répertoriées dans la matrice de compatibilité des produits.  Les nouvelles fonctionnalités sont testées de manière approfondie et les fonctionnalités existantes sont également testées pour prévenir les régressions.

### Mise en production des logiciels

Une fois confié officiellement aux services CO de Skillsoft, l’ensemble logiciel est examiné par ces services qui décident alors d’une stratégie de déploiement.  Le logiciel passe alors dans un cycle de publication contrôlé en étant déployé dans un environnement de préproduction.  Après vérification dans l’environnement de préproduction, l’ensemble logiciel est déployé à la production. L’architecture de micro-services permet de déployer les logiciels de façon rapide et transparente.

### Gestion des correctifs et des versions

Les améliorations continues apportées aux logiciels font parfois que les correctifs sont disponibles dans les lignes de produits logiciels de Skillsoft.  Toutes les versions logicielles, mineures et majeures, y compris les correctifs sont uniques et cette version est transparente pour tous les opérateurs.  La stratégie de publication des déploiements de correctifs copie celle du processus de publication des logiciels décrite ci-dessus.

## Ingénierie logicielle – Contrôle des modifications

### Processus d'ingénierie logicielle

Une fois les spécifications fonctionnelles finalisées, l'architecte logiciel du produit et un architecte DevOps CO attribué à chaque équipe déterminent l'architecture logicielle générale. Dans certains cas, des considérations d'architecture peuvent entraîner la modification des spécifications fonctionnelles. Ces modifications seront signifiées aux parties concernées, puis seront déterminées une spécification et une architecture fonctionnelles finales. Cette architecture est documentée et envoyée au responsable DevOps pour examen, définition de la portée du projet et attribution des ressources.

### Accès au code source

L'accès à tous les logiciels et leurs versions est strictement contrôlé avec Github, une solution de contrôle de source logicielle. L'accès au code source est fourni selon les besoins et est restreint à l'équipe d'ingénierie logicielle de Skillsoft.

### Processus de publication des logiciels

Seul le responsable DevOps en charge de la ligne de produits peut envoyer le logiciel de l'ingénierie logicielle à l'assurance qualité. Seul l'ingénieur de contrôle qualité assigné a l'autorité d'envoyer le logiciel des systèmes d'assurance qualité aux systèmes de qualification finale, à condition que le logiciel remplisse les critères d'acceptation prédéfinis pour la publication. Seul l'ingénieur de contrôle qualité assigné (avec l'approbation du responsable Contrôle qualité) a l'autorité d'envoyer le logiciel de la qualification finale aux services CO de Skillsoft, à condition que le logiciel remplisse les critères d'acceptation prédéfinis pour la publication générale.

## Gestion des correctifs – Description du processus

### Logiciel

Une suite logicielle de gestion centralisée des correctifs garantit une posture de sécurité cohérente sur tous les systèmes gérés. Les services CO de Skillsoft ont, par là même, les moyens de réagir activement aux menaces émergentes. Tous les correctifs logiciels disponibles sont examinés par les architectes CO et déployés selon un calendrier défini par les risques associés.

### Appareils réseau et de sécurité

Une équipe de professionnels du réseau et de la sécurité dédiée examinent continuellement les nouveaux correctifs et améliorations disponibles pour les appareils réseau et de sécurité.  Les lots de signatures pour les appareils de détection et de prévention des intrusions sont téléchargés quotidiennement et examinés pour implémentation en permanence.

## Contrôles de compte

### Accès aux systèmes

L'accès à tous les systèmes de cloud privé est limité au personnel des services CO de Skillsoft.  Dans certains cas, des techniciens agréés par les fournisseurs se voient accorder un accès aux systèmes lors de défaillances matérielles ou de l'implication de services professionnels.

### Gestion des accès

Le contrôle de l'accès aux systèmes et aux sites est contrôlé par un groupe restreint d'employés des services CO de Skillsoft.  L'accès aux systèmes est accordé à un niveau correspondant au poste de la personne.  L'accès aux appareils réseau et de sécurité est limité à l'équipe de gestion réseau, au directeur CO et à l'architecte CO principal.  L'accès au site du cloud privé est géré en collaboration avec le fournisseur de services de colocalisation via une liste de contrôle d'accès officielle.  La gestion de cette liste est limitée aux responsables CO.

## Défenses du périmètre

### Pare-feu

Skillsoft a sélectionné les meilleures solutions logicielles et matérielles auprès des leaders du secteur.  Les pare-feu utilisent une stratégie très restrictive filtrant uniquement le trafic connu et l'accès requis aux ports.  L'accès aux systèmes de pare-feu est strictement contrôlé et les réglages effectués sur les stratégies de pare-feu sont soumises à l'approbation de la direction avant toute implémentation.

### Détection et prévention des intrusions

Grâce à la corrélation des événements et à la recherche granulaire de signatures prédéterminées, Skillsoft fournit une protection complète contre les vulnérabilités connues et une défense zero-day contre les nouvelles menaces.

Les signatures des systèmes de détection et de prévention des intrusions sont examinées et mises à jour en permanence.

### Système de prévention des intrusions

L'implémentation active et redondante d'un système de prévention des intrusions est une protection efficace et éprouvée contre les attaques par force brute et de déni de service. Les réglages apportés à la configuration du système de prévention des intrusions sont examinés en permanence.

### Connexion à l'internet public

L'application SaaS Percipio est disponible sur l'internet public. Des mesures ont été toutefois mises en place pour empêcher les accès non autorisés à l'application SaaS. Cela inclut l'accès uniquement par nom d'utilisateur et mot de passe à votre site Percipio et la possibilité pour les clients de gérer eux-mêmes leurs comptes d'application conformément à leurs propres stratégies grâce à l'interface d'administrateur d'apprentissage. Le client peut choisir de mettre en place l'authentification unique (SSO) pour garantir une meilleure protection et une utilisation facile à ses utilisateurs.

## Protection de la piste d'audit

### Gestion des fichiers journaux

La journalisation système intense capture tous les événements relatifs à l'accès système, notamment l'utilisation de droits d'utilisateur privilégié, les démarrages/arrêts de service, les connexions et les déconnexions. Les fichiers journaux de renseignements réseau et pare-feu capturent tous les événements d'échec d'accès et toutes les activités suspectes tels que définis dans notre infrastructure de détection et de prévention des intrusions. La journalisation système exhaustive et la journalisation de la gestion de stockage/SANS consignent les événements non standard. Les fichiers journaux détaillés des applications enregistrent tous les événements d'application inhabituels en plus des fichiers journaux détaillés des serveurs web. Les services CO de Skillsoft conservent tous les fichiers journaux d'accès, de sécurité et système pour une durée indéterminée. Tous les journaux d'événements sont archivés quotidiennement sur un stockage sur disque centralisé pour pouvoir y accéder facilement. Ce référentiel centralisé est ensuite enregistré sur bande et conservé conformément à nos politiques de rétention des bandes telles que définies dans ce document. L'accès aux fichiers journaux est limité au personnel CO, sauf les fichiers journaux web et d'erreurs d'application qui sont partagés, selon les besoins, avec l'équipe d'ingénierie logicielle de Skillsoft.

### Signalement aux client d'une brèche de sécurité

Skillsoft suit un processus de gestion des incidents strict, approuvé par ses clients fédéraux et ses clients associés au ministère de la défense américaine. Si un incident de sécurité survient : les informations relatives à l'incident seront fournies par l'assistance technique de Skillsoft au contact principal du client. La première phase de contact sera d'indiquer qu'il y a eu un problème et le statut de la correction. Les mises à jour suivantes seront envoyées lors du processus de correction. Une fois l'incident résolu, le service CO effectue une analyse des causes fondamentales. Les résultats seront fournis aux clients sur demande.

## Protection et conservation des données

### Données des clients – Stockage

Toutes les données des clients sont stockées sur une baie de stockage d'entreprise fournissant un niveau de protection et d'intégrité des données maximum. Elles sont stockées uniquement dans des bases de données relationnelles sans aucune donnée présente sur les systèmes web accessibles sur l'internet. L'accès à ces données est limité au personnel CO. Les données des clients sont dupliquées sur le site de récupération après sinistre du cloud privé, qui est également géré de façon rigoureuse par Iron Mountain. Elles sont sauvegardées quotidiennement et transférées de manière sécurisée sur des bandes chiffrées vers une installation hors site gérée par Iron Mountain. Dans certains cas, les données clients sont dupliquées dans un environnement de laboratoire contrôlé et sécurisé pour résoudre des problèmes ou pour des exercices de planification des capacités directement liés au client. Les données dupliquées utilisées dans cet environnement sont soumises à un nettoyage de base de données qui supprime toutes les informations personnelles des données avant leur utilisation en laboratoire. Pour garantir la confidentialité et la sécurité des données, le processus de nettoyage s'effectue dans l'environnement de cloud privé avant l'exportation des données vers le laboratoire.

### Données des clients – Protection

L'accès aux systèmes de bases de données et aux bases de données des clients est limité au personnel CO. L'accès distant privilégié se fait exclusivement via un canal chiffré et sécurisé. Les sauvegardes sur bande sont confiées à une autorité en matière de stockage de données et de bandes (Iron Mountain). Les supports sont stockés dans une installation sécurisée et distante qui n'est accessible qu'à un groupe restreint des services CO.

### Stockage des mots de passe

Les mots de passe des comptes d'utilisateur des clients sont hachés (et salés) de manière sécurisée avec bcrypt

### Méthodes d'accès pour l'utilisateur final

Tous les accès aux données se font via des systèmes web accessibles publiquement et protégés par un mot de passe. L'accès direct aux données n'est pas autorisé.

## Gestion du personnel

### Rôles et responsabilités

Skillsoft a constitué une équipe hors pair de professionnels de l'informatique dans une structure organisationnelle indiquant clairement la hiérarchie des responsabilités, de supervision et de propriété sans sacrifier l'agilité et la réactivité requises par les clients.  L'équipe des services CO est généralement divisée selon les équipes suivantes :

- Réseau et sécurité
- Architectes de systèmes
- Administrateurs des systèmes et applications
- Administrateurs des bases de données et du stockage des données
- Assistance du produit et approvisionnement des clients
- Gestion des programmes

### Vérification des antécédents des employés

Skillsoft a conscience de la sensibilité des données traitées par les employés CO. Pour garantir la meilleure sensibilisation à la sécurité et une diligence raisonnable, Skillsoft vérifie les antécédents (opération soumise aux réglementations locales applicables) des employés potentiels pour des postes prédéterminés qui requièrent un accès aux données client. Skillsoft vérifie également les références fournies par les candidats lors du processus de candidature. De plus, tous les employés CO doivent lire et signer une politique de confidentialité et de sécurité détaillant les rôles et responsabilités, les procédures d'escalade et le code de conduite global de l'organisation CO. Tous les employés CO doivent signer cette politique tous les ans pour signifier qu'ils la comprennent et s'engagent à respecter ses directives.

### Équipe CO dédiée

Skillsoft a conscience des défis uniques que rencontrent les prestataires de services et des compétences spécialisées requises pour gérer et développer des infrastructures cloud de manière efficace.  Pour répondre à ces défis, Skillsoft a donc investi fortement dans une équipe de services CO dédiée qui a pour seul mandat de garantir la meilleur expérience possible à nos clients.

### Description des expertises

Les services CO de Skillsoft sont formés de professionnels expérimentés et compétents.  En plus de leurs années d'expérience, de nombreux employés des services CO possèdent également des certifications venant des autorités du secteur suivantes :

- Cisco
- RedHat
- DevOps
- CheckPoint
- EMC
- GIAC
- VMWare
- CommVault
- AWS Cloud Practitioner

### Formation du personnel

Les technologies évoluant sans cesse, Skillsoft est conscient du rôle essentiel que joue de la formation dans la prestation réussie de services.  Pour garantir que Skillsoft a les meilleures ressources possibles à disposition de ses clients, Skillsoft consacre beaucoup de temps aux formations sur tous les produits de l'infrastructure du cloud privé. Un programme de formation officiel a été élaboré pour les produits propriétaires de Skillsoft et des cours généraux sur la confidentialité et la sécurité sont assignés aux employés tous les ans.

## Gestion des capacités

Skillsoft prend la gestion de projet très au sérieux afin de s'assurer que les ressources nécessaires sont disponibles pour les nouveaux produits, les nouveaux clients, les mises à niveau clients et le remplacement des systèmes. L'application Percipio fait l'objet d'un test de charge qui valide les exigences matérielles et que la configuration de déploiement répond à la demande de nos clients.

L'application Percipio est déployée selon un plan de déploiement prédéfini qui décrit exactement comment Percipio partage le matériel et comment ce matériel est configuré. L'infrastructure requise est préconçue et configurée à partir de fiches techniques et d'images préconfigurées créées par les architectes de systèmes. L'environnement de cloud privé existant est surveillé en permanence pour vérifier l'utilisation des ressources. Lorsque des situations d'urgence se produisent, l'équipe CO a des capacités redondantes prêtes à être déployées via la configuration pour répondre à tout problème de capacité pouvant émerger.

## Fournisseurs de services tiers

### Fastly

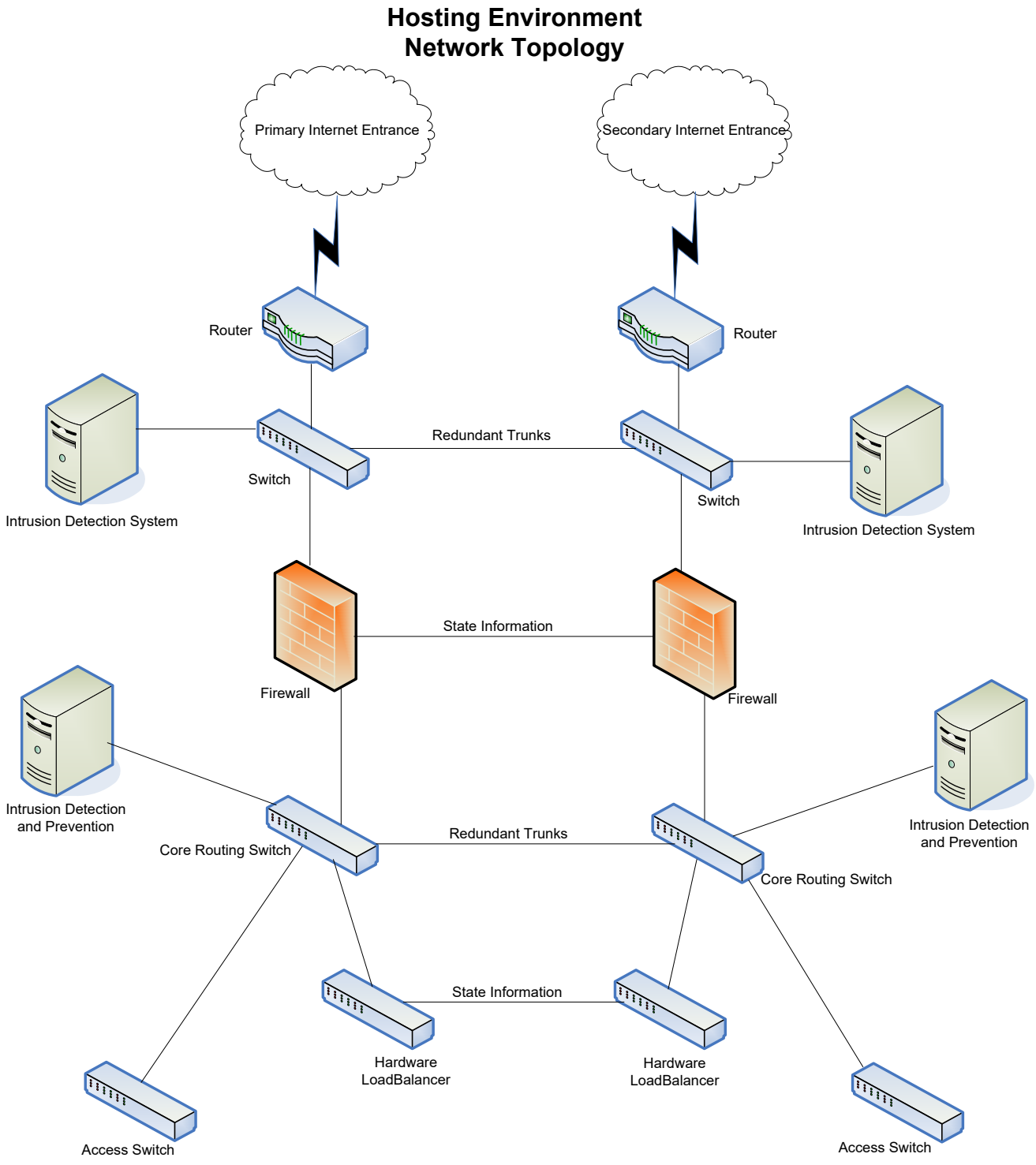
Skillsoft utilise les services Fastly pour la diffusion de vidéos sur Percipio.

https://www.fastly.com

### Stockage hors site Iron Mountain

Skillsoft utilise Iron Mountain pour son stockage de sauvegardes hors site. Iron Mountain est responsable du transport et du stockage sécurisés des supports de sauvegarde. Le site d'Iron Mountain se trouve à Francfort en Allemagne.

# Annexe B – Topologie Percipio


Hosting Environment
Network Topology
Primary Internet Entrance
Secondary Internet Entrance
Router
Router
Intrusion Detection System
Switch
Redundant Trunks
Switch
Intrusion Detection System
Firewall
State Information
Firewall
Intrusion Detection
and Prevention
Core Routing Switch
Redundant Trunks
Core Routing Switch
Intrusion Detection
and Prevention
State Information
Hardware
LoadBalancer
Hardware
LoadBalancer
Access Switch
Access Switch