INTÉGRITÉ DES PROCESSUS ET SÉCURITÉ DE L'INFORMATION

SSAE 18 et ISAE 3402 sont des normes internationales qui analysent le niveau de contrôle des entreprises vis-à-vis des technologies de l'information et des processus associés. La conformité avec ces normes indique que les processus, procédures et contrôles ont été évalués et testés de manière formelle.

A propos des normes SSAE 18 et ISAE 3402

La norme SSAE 18, instaurée par le Conseil des Normes d'Audit (Auditing Standards Board) de l'AICPA (American Institute of Certified Public Accountant), est une approche complète et élargie du rapport de conformité. SSAE 18 reflète et respecte étroitement ISAE 3402, la première norme internationale pour les prestataires de service. Développée pour répondre au besoin de normes indépendantes au niveau international, ISAE 3402 fournit un dispositif de contrôles destiné à donner plus d'uniformité et de transparence lors d'audits au sein d'entreprises prestataires de services.

SSAE 18 et ISAE 3402 remplacent l'ancienne norme SAS 70 (Statement on Auditing Standards 70) et sont devenus les standards en matière de contrôle dans les entreprises de services. Ils attestent de la fiabilité des procédures de contrôle mises en place et permettent aux sociétés de services de garantir l'intégrité de leurs processus auprès de leurs clients.

En respectant ces normes, les prestataires de services peuvent offrir à leurs clients un outil précieux de planification et de rationalisation de l'audit de leurs états financiers. Les normes SSAE 18 et ISAE 3402 faisant autorité, elles permettent aux sociétés de services de dévoiler leurs activités et processus de contrôle auprès de leurs clients et des auditeurs de leurs clients, en utilisant un format de rapport uniforme.

SSAE 18 and ISAE 3402 sont ainsi principalement utilisées par les entreprises dont les missions impactent les finances de leurs clients (gestionnaires de paie, centres de traitement informatique, tiers de confiance, logisticiens, administrateurs de fond, etc…).

Type 1 versus Type 2

Les normes SSAE 18 et ISAE 3402 Type 1 attestent de la fiabilité des procédures de contrôle de l'entreprise. Pour la plupart des entreprises, ces normes de Type 1 représentent une première étape de ce qui est souhaité à terme, à savoir les normes de type 2. Les rapports de Type 2 incluent les mêmes étapes mais ils attestent, en sus, l'efficacité du fonctionnement des contrôles pour une période d'au moins 6 mois consécutifs. Les normes de Type 2 attestent donc d'une part que les systèmes de contrôle de l'entreprise ont été correctement définis, mais aussi que la fiabilité et l'efficacité du fonctionnement des contrôles ont été testées de manière approfondies.

Amélioration de la sécurité et de la protection des données privées

Les certifications ont pris de plus en plus d'importance ces dernières années dans la mesure où les entreprises essaient de répondre à des règlementations de plus en plus exigeantes. De nouvelles règlementations sur la détention et le traitement de données sont apparues suite à des scandales financiers et à l'inquiétude de l'opinion publique concernant la sécurité et la confidentialité des informations personnelles.

De plus, l'augmentation des pratiques d'externalisation a démontré encore plus la nécessité des normes SSAE 18 et ISAE 3402, dans la mesure où les prestataires de service doivent prouver l'existence de contrôles adéquats lorsqu'ils hébergent ou traitent des données appartenant à leurs clients.

La loi Sarbanes-Oxley est un exemple de législation qui a un fort impact sur les processus d'audit et de reporting des entreprises. Sarbanes-Oxley définit une responsabilité sociétale vis-à-vis du reporting financier et précise que les dirigeants d'une entreprise doivent publier des évaluations de l'efficacité des contrôles et procédures internes. SSAE 18 et ISAE 3402 répondent aux règles de contrôle interne soulignées dans cette loi.

Niveau de conformité d'Esker

Déjà conforme aux exigences des normes de Type 1 depuis 2012, Esker a été déclaré conforme aux normes Type 2 en 2014 par le cabinet d'audit indépendant A-lign ce qui permet de garantir un niveau de sécurité accru et de rassurer les clients en mode SaaS.

Partout à travers le monde, des entreprises font confiance à Esker pour héberger et traiter leurs documents de gestion et leurs données financières. Ces normes garantissent de la transparence aux clients, renforcent la confiance et confèrent à Esker un réel avantage concurrentiel, surtout en Europe où Esker est l'un des seuls prestataires à être en conformité.

Objectifs de contrôle

Esker a investi du temps et des ressources afin d'être conforme à ces normes et de répondre à plusieurs objectifs de contrôle incluant ceux listés ci-dessous.

Organisation et administration – La structure organisationnelle d'Esker permet une division appropriée des responsabilités afin de communiquer efficacement et de séparer les fonctions et devoirs de la prestation de services (procédures formalisées pour l'embauche de nouveaux employés, les descriptions de poste, les exigences de formation, etc.).

Sécurité physique et protection de l'environnement – Les data centers d'Esker sont des zones contrôlées et à accès restreint, surveillées par du personnel d'une société tierce et grâce à du matériel vidéo, permettant une surveillance 24h/24, 7j/7. La protection de l'environnement inclut : architecture avec des faux-planchers pour éviter les dégâts des eaux, climatisation avec des contrôles réguliers, système d'alerte de détection incendie précoce, et d'extinction évolué du feu,

un système d'évacuation des gaz, et politiques de sécurité régulièrement mises à jour et testées.

Sécurité logique – Les comptes utilisateurs pour se connecter aux systèmes informatiques d'Esker sont uniques et nominatifs, et une politique complexe de mot de passe a été mise en application. L'accès interne est limité aux employés d'Esker autorisés.

Développement d'applications et gestion du changement – Tous les changements, incluant la maintenance d'urgence et les fixes de la solution ou de l'infrastructure Esker on Demand sont correctement autorisés, testés, mis en œuvre et documentés. Les équipes Esker dédiées au développement écrivent les spécifications et développent de nouvelles fonctionnalités, des corrections et des améliorations sur tous les produits on Demand d'Esker.

Gestion des incidents – Esker est équipé d'un outil d'administration automatisé destiné à gérer les incidents. Cet outil permet à Esker de suivre un incident depuis sa soumission jusqu'à sa clôture de s'assurer que les problèmes de systèmes sont enregistrés, analysés et résolus correctement dans les temps dévolus.

Gestion des données – Les systèmes d'Esker sont sauvegardés périodiquement, sur la base d'exigences de données identifiées, et des procédures sont mises en place afin de maintenir la confidentialité et l'intégrité du media de sauvegarde.

Monitoring et reporting – Un système automatique de reporting contrôle de manière permanente les opérations Esker on Demand et centralise les événements dans un tableau de bord de contrôle. Ce système assure que le document du client a bien été reçu et traité correctement dans le délai convenu. Des équipes internationales sont organisées de manière à assurer un contrôle 24h/24, 7j/7, 365 jours par an et de pouvoir agir en conséquence.

Pour atteindre ces objectifs de contrôle, de nombreux contrôles internes ont été mis en place, tels que :

- Sécurité des data centers,
- Contrôle de l'infrastructure,
- Accès logistiques,
- Opérations informatiques fiables (sauvegarde, reporting, archivage et disponibilité du système), et
- Recrutement.

Les avantages des normes SSAE 18 et ISAE 3402

Du point de vue du prestataire de service

Bien que les rapports SSAE 18 et ISAE 3402 puissent être coûteux et chronophages, ils offrent des avantages indéniables au prestataire de service qui les utilise. L'un des principaux bénéfices est qu'ils procurent de la transparence et ils permettent l'établissement d'une relation de confiance avec les clients grâce à des contrôles et des opérations indépendants vérifiés par un tiers impartial.

Du point de vue de l'entreprise utilisatrice (client)

Les rapports SSAE 18 et ISAE 3402 sont intéressants pour les entreprises utilisatrices car ils donnent accès aux contrôles et sauvegardes du prestataire de service. Les rapports que les entreprises utilisatrices reçoivent décrivent de manière très détaillée les contrôles spécifiques du prestataire de service.

De plus, ces rapports permettent à l'entreprise utilisatrice de réaliser des économies dans la mesure où elle n'aura plus besoin d'envoyer ses propres auditeurs chez le prestataire de service.

Ces normes sont un acte gagnant-gagnant pour les prestataires de service et pour leurs clients, délivrant de nombreux avantages pour chacune des parties impliquées. Pour le prestataire de service, les normes SSAE 18 et ISAE 3402 sont un moyen de prouver sa compétence à instaurer des contrôles et des sauvegardes internes, de le différencier des autres acteurs du marché et de démontrer clairement un avantage concurrentiel. Pour les clients, SSAE 18 et ISAE 3402 leur permettent de s'assurer que leurs informations sont gérées de manière totalement sécurisée et transparente.

©2017 Esker S.A. Tous droits réservés. Esker et le logo Esker sont des marques commerciales de Esker. Toutes les autres marques mentionnées dans ce document appartiennent à leurs propriétaires respectifs.

ESKER®
Document Process Automation

Esker SA
113 Boulevard de Stalingrad
69100 Villeurbanne
Tél. : +33 (0)4 72 83 46 46 — Fax : +33 (0)4 72 83 46 40
info@esker.fr — www.esker.fr

Suivez-nous