Annexe : Audit de Sécurité

Mises à jour le 24 janvier 2025

Résumé des Points Essentiels

Ce résumé est fourni à titre indicatif pour faciliter la lisibilité du présent document.

L'audit de sécurité évalue les systèmes et infrastructures pour identifier les vulnérabilités et proposer des solutions. Le périmètre est défini par contrat, et toute extension nécessite un accord. Le rapport inclut les failles détectées et des recommandations, valables 3 mois. Le Client est responsable de l'accès aux systèmes, des sauvegardes avant l'audit, et de l'application des recommandations. La confidentialité des résultats est garantie, et les frais restent dus selon les termes convenus.

Table des matières

Payette Jean (EI) | 10 de la Mare Boutillier – 77166 – Grisy-Suisnes | Tél : 07 56 81 89 12
Siret : 753 004 589 | Site web : www.owlsystems.fr | Email : service-client@owlsystems.fr

Section 1 Objet de l'audit de sécurité

L'audit de sécurité a pour objectif d’évaluer la sécurité des systèmes, applications, réseaux, et infrastructures sous gestion du Client, dans le but d'identifier les vulnérabilités existantes et de fournir un ensemble de recommandations pour améliorer la sécurité globale.

L'audit inclut l'examen des éléments suivants, sans s'y limiter :

- Les configurations système et les pratiques de gestion des accès,
- Les protections des données sensibles,
- Les mécanismes de défense contre les attaques externes,
- L'évaluation de la sécurité des applications et des infrastructures réseaux, y compris la vérification des systèmes de contrôle d'accès, des politiques de sécurité et de la configuration des serveurs.

Le Prestataire s'engage à mener l'audit conformément aux meilleures pratiques en matière de sécurité informatique. Cependant, toute extension du périmètre de l'audit, c’est-à-dire l'analyse d'éléments ou de processus non spécifiquement mentionnés dans le devis ou le contrat initial, nécessitera l'accord préalable du Client et pourra entraîner des frais supplémentaires, conformément à un devis révisé.

Section 2 Périmètre de l'audit de sécurité

L'audit de sécurité est réalisé sur le périmètre spécifié dans le Devis ou le Contrat. Toute extension du périmètre doit faire l'objet d'un devis supplémentaire et d'une acceptation par les deux parties.

Dans le cadre de l'audit, le Prestataire peut être amené à explorer plus en profondeur certaines zones, y compris celles qui n'ont pas été explicitement définies dans le périmètre initial, si des vulnérabilités significatives sont détectées. Cette exploration est réalisée de manière professionnelle et dans l'intérêt de renforcer la sécurité globale du système, mais cela ne constitue pas une extension formelle du périmètre de l'audit, sauf accord écrit préalable.

L'audit peut inclure, sans s'y limiter :

- Analyse des systèmes et infrastructures réseaux.
- Vérification des pratiques de gestion des accès et des mots de passe.
- Évaluation de la configuration des serveurs et des applications.
- Tests d'intrusion (en fonction de l'accord avec le Client).
- Revue des politiques de sécurité internes et des procédures de gestion des incidents.

Le Prestataire ne pourra pas être pénalisé pour des actions d'investigation supplémentaires entreprises dans le cadre de l'audit, si elles s'avèrent nécessaires

Payette Jean (EI) | 10 de la Mare Boutillier – 77166 – Grisy-Suisnes | Tél : 07 56 81 89 12
Siret : 753 004 589 | Site web : www.owlsystems.fr | Email : service-client@owlsystems.fr

pour la détection de vulnérabilités et la protection des systèmes. Toutefois, si ces investigations nécessitent une extension du périmètre ou génèrent des coûts additionnels, un devis révisé sera soumis et devra être accepté par le Client avant d'entreprendre toute action supplémentaire.

Section 3 Méthodologie de l'audit

Les tests seront réalisés conformément aux meilleures pratiques de sécurité et de manière non destructive dans la mesure du possible, afin de ne pas perturber les activités normales du Client. Cependant, le Prestataire ne pourra être tenu responsable de toute perturbation, qu'elle soit mineure, majeure ou imprévue, directement ou indirectement causée par les tests réalisés dans le cadre de l'audit.

Cela inclut, mais ne se limite pas à :

- L'interruption de services,
- La dégradation des performances des systèmes,
- Le redémarrage non prévu des systèmes,
- Toute autre perturbation dans le fonctionnement des infrastructures informatiques du Client, même si elles résultent des tests de pénétration, des scans de vulnérabilité, ou des autres évaluations effectuées pendant l'audit.

Le Client reconnaît que ces tests peuvent, dans certains cas, provoquer des incidents imprévus dus à la présence de vulnérabilités non détectées ou à la réaction des systèmes à des attaques simulées, telles que des resets ou des coupures de service. Le Client accepte d’assumer la pleine responsabilité de la gestion des risques associés et garantit avoir pris les mesures appropriées pour se protéger contre de telles éventualités.

Le Prestataire ne pourra être tenu responsable des dommages, pertes ou interruptions de services découlant des tests, et ce, même en cas de perturbation importante des systèmes ou d’incidents imprévus causés par des vulnérabilités découvertes durant l'audit.

Section 4 Rapport d'audit et recommandations

À la suite de l'audit, le Prestataire fournira un rapport détaillé comprenant :

- Une description des vulnérabilités identifiées.
- Des recommandations pour corriger les failles de sécurité.
- Des priorités d'action selon la gravité des vulnérabilités.

Le rapport sera remis dans un délai de 15 jours après la fin de l'audit, sauf en cas de circonstances exceptionnelles, auquel cas le Prestataire s'engage à informer le Client sans délai du retard et de ses raisons. Le délai de remise du rapport est indicatif, et aucun recours ni pénalité ne sera appliqué en cas de retard, sauf si ce retard excède une durée raisonnable ou résulte d'une faute manifeste du

Payette Jean (EI) | 10 de la Mare Boutillier – 77166 – Grisy-Suisnes | Tél : 07 56 81 89 12
Siret : 753 004 589 | Site web : www.owlsystems.fr | Email : service-client@owlsystems.fr

Prestataire.

Section 5 Responsabilités du Prestataire

Le Prestataire s'engage à réaliser l'audit de manière professionnelle, conformément aux meilleures pratiques de l'industrie. Cependant, il est important de souligner qu'il est impossible de garantir la sécurité à long terme des systèmes, car la sécurité des infrastructures informatiques dépend de nombreux facteurs en constante évolution, notamment des actions des utilisateurs, des mises à jour système, des attaques externes et de l'évolution des technologies.

Ainsi, bien que le Prestataire fournisse un ensemble de recommandations visant à améliorer la sécurité, le Client est seul responsable de la mise en œuvre complète et correcte de ces recommandations. Si le Client ne met pas en œuvre ces recommandations dans les délais spécifiés, le Prestataire ne pourra en aucun cas être tenu responsable des failles de sécurité qui apparaîtraient après l'audit, ni des dommages qui en découleraient.

Section 6 Responsabilités du Client

Le Client s'engage à mettre en œuvre toutes les recommandations formulées dans le rapport d'audit dans les délais spécifiés. En cas de non-application partielle ou totale de ces recommandations, le Prestataire ne pourra être tenu responsable des failles de sécurité qui apparaîtraient après l'audit. Le Client reconnaît que la sécurité des systèmes est un processus continu, et que l'inaction face aux vulnérabilités identifiées pourrait entraîner des risques et des incidents qui ne pourront en aucun cas être attribués au Prestataire.

a) Types d'audit et niveaux d'accès

Audit avec accès complet ("White-box testing") : Le Client doit fournir au Prestataire un accès complet à ses systèmes, infrastructures et informations pertinentes. Cela comprend l'accès aux serveurs, réseaux, bases de données, applications et tout autre élément nécessaire à la réalisation complète de l'audit. En cas de refus d'accès, d'obstruction ou de restriction d'accès à des informations critiques, le Prestataire se réserve le droit de suspendre ou d'interrompre l'audit sans que le Client puisse prétendre à une réduction de prix ou à une annulation de la prestation. Dans ce cas, le Client restera redevable des frais convenus pour l'audit, dans les conditions stipulées dans le Devis ou le Contrat.

Audit avec accès partiel ("Gray-box testing") : Si le Client décide de limiter l'accès aux systèmes, l'audit sera restreint aux zones accessibles. Dans ce cas, le Prestataire ne pourra pas garantir que toutes les vulnérabilités possibles ont été identifiées. Le Client reconnaît que certaines zones critiques pourraient ne pas être couvertes, et que des vulnérabilités importantes pourraient être omises. Le Client

Payette Jean (EI) | 10 de la Mare Boutillier – 77166 – Grisy-Suisnes | Tél : 07 56 81 89 12
Siret : 753 004 589 | Site web : www.owlsystems.fr | Email : service-client@owlsystems.fr

assume la responsabilité des risques associés à la non-couverture de ces zones et accepte de ne pas tenir le Prestataire responsable si des failles sont découvertes après l'audit dans des zones non auditées.

Audit sans accès direct ("Black-box testing") : Dans le cadre d'un audit sans accès direct, le Prestataire réalise un audit en ne disposant d'aucune information préalable ou d'accès privilégié aux systèmes et infrastructures du Client. Ce type d'audit est réalisé de manière purement externe, dans le but d'évaluer les vulnérabilités visibles depuis l'extérieur de l'entreprise. Le Client reconnaît que, en raison du manque d'accès aux informations internes, ce type d'audit présente des limitations évidentes, et des vulnérabilités critiques qui ne sont pas exposées à l'extérieur du système peuvent ne pas être identifiées. Le Client accepte les risques associés à ce type de test et comprend que la couverture des systèmes pourrait être partielle. Le Client renonce également à toute réclamation si des failles sont découvertes dans des zones non auditées ou non accessibles dans ce contexte.

b) Obligations supplémentaires du Client

Indépendamment du type d'audit, le Client est responsable de la mise en œuvre des recommandations formulées dans le rapport d'audit. En cas de non-application de ces recommandations dans les délais spécifiés, le Prestataire ne pourra en aucun cas être tenu responsable des failles de sécurité qui apparaîtraient après l'audit. Le Client reconnaît que la sécurité des systèmes est un processus continu, et que l'inaction face aux vulnérabilités identifiées pourrait entraîner des risques qui ne pourront être attribués au Prestataire.

Le Client est également responsable de la mise en œuvre des actions nécessaires pour maintenir la sécurité de ses systèmes après l'audit, incluant la mise à jour régulière des systèmes et l'application des correctifs de sécurité.

Section 7 Limitation de la Responsabilité

Le Prestataire ne pourra être tenu responsable des conséquences découlant de l'exploitation de vulnérabilités après l'audit, dès lors que ces vulnérabilités n'ont pas été corrigées par le Client conformément aux recommandations fournies dans le rapport d'audit.

Le Client reconnaît que la sécurité des systèmes est un processus dynamique et que, même si toutes les recommandations sont appliquées, de nouvelles vulnérabilités peuvent apparaître à tout moment en raison de changements dans l'environnement informatique, des actions des utilisateurs ou de l'évolution des menaces.

Le Prestataire ne peut garantir l'absence de nouvelles failles de sécurité après l'audit, car la sécurité est en constante évolution. En conséquence, le Client accepte d’être responsable de la mise à jour continue de ses systèmes, de l’application régulière des recommandations de sécurité et de la réévaluation proactive de la

Payette Jean (EI) | 10 de la Mare Boutillier – 77166 – Grisy-Suisnes | Tél : 07 56 81 89 12
Siret : 753 004 589 | Site web : www.owlsystems.fr | Email : service-client@owlsystems.fr

sécurité de ses systèmes, afin de prévenir les risques liés à de potentielles nouvelles menaces.

a) Responsabilité pour Dommages Indirects Post-Audit

Le Prestataire ne pourra en aucun cas être tenu responsable des vulnérabilités, failles ou problèmes de sécurité qui :

- N'étaient pas détectables avec les moyens et méthodes d'audit utilisés au moment de l'intervention
- Sont apparus après la réalisation de l'audit du fait de l'évolution des menaces ou des systèmes
- Résultent de modifications apportées aux systèmes après l'audit
- N'ont pas fait l'objet d'une correction par le Client malgré leur signalement dans le rapport d'audit

b) Confidentialité des Résultats

Le rapport d'audit et l'ensemble des informations recueillies sont strictement confidentiels et :

- Ne peuvent être communiqués à des tiers sans l'accord écrit préalable du Client
- Doivent être protégés par des mesures de sécurité appropriées
- Doivent être détruits ou restitués au Client à sa demande à l'issue de la mission
- Ne peuvent être utilisés que dans le cadre strict de la mission d'audit

Le Client s'engage également à maintenir la confidentialité sur les méthodes et outils utilisés par le Prestataire."

Section 8 Confidentialité

Les informations recueillies au cours de l'audit de sécurité seront traitées conformément à la Section XI des Conditions Générales de Vente (CGV) du Prestataire, qui régit la confidentialité des données et des informations du Client.

Le Prestataire s'engage à :

- - Chiffrer systématiquement les données d'audit
- - Limiter l'accès aux seuls intervenants nécessaires
- - Supprimer les données brutes dans un délai de 30 jours après livraison du rapport final

Payette Jean (EI) | 10 de la Mare Boutillier – 77166 – Grisy-Suisnes | Tél : 07 56 81 89 12
Siret : 753 004 589 | Site web : www.owlsystems.fr | Email : service-client@owlsystems.fr

- - Ne jamais utiliser les informations découvertes à d'autres fins que l'audit
- - Notifier immédiatement le Client en cas de compromission suspectée des données

Le Client autorise le Prestataire à conserver une copie archivée du rapport final pendant 3 ans pour des besoins de traçabilité.

Le Prestataire s'engage à ne pas divulguer ces informations à des tiers sans le consentement préalable du Client, sauf si la loi l'exige. Les résultats de l'audit, y compris les vulnérabilités identifiées et les recommandations, seront partagés exclusivement avec le Client, sauf accord préalable stipulant autrement.

Section 9 Conditions de Facturation

Les frais de l'audit de sécurité sont définis dans le Devis ou le Contrat signé entre les parties. Le Client s'engage à régler ces frais dans les délais convenus, indépendamment de l'acceptation ou du rejet des résultats de l'audit.

Le Client reconnaît que, même en cas de désaccord sur les résultats de l'audit, les frais de l'audit restent dus conformément aux modalités de paiement spécifiées dans le Devis ou le Contrat. Toutefois, si le Client considère que l'audit ne répond pas à ses attentes ou qu'il y a une divergence substantielle dans les résultats, il pourra demander une révision du rapport.

Cette révision sera effectuée par le Prestataire dans un délai raisonnable, et les frais associés à cette révision seront facturés en supplément, sauf si le Prestataire reconnaît un manquement dans la réalisation de l'audit.

En cas de révision, les parties s'engagent à discuter de manière constructive pour parvenir à un accord sur les modifications éventuelles du rapport d'audit, tout en respectant la limite de responsabilité du Prestataire spécifiée dans le contrat. Si aucune solution amiable n'est trouvée, le Client reste tenu de régler les montants dus pour l'audit initial, sans préjudice de tout recours légal ultérieur.

Si des modifications ou des ajouts sont nécessaires pendant l'audit, le Client accepte que des frais supplémentaires soient facturés pour ces services additionnels.

Section 10 Validité de l'Audit

L'audit de sécurité effectué par le Prestataire constitue une évaluation ponctuelle de la sécurité des systèmes, des infrastructures et des pratiques du Client, à un instant donné. En raison de la nature évolutive des menaces informatiques, des vulnérabilités peuvent émerger après l'audit en raison de diverses causes, telles que les mises à jour logicielles, les modifications de l'infrastructure ou l'apparition de nouvelles attaques.

Les résultats de l'audit sont donc valables pour une période maximale de trois (3)

Payette Jean (EI) | 10 de la Mare Boutillier – 77166 – Grisy-Suisnes | Tél : 07 56 81 89 12
Siret : 753 004 589 | Site web : www.owlsystems.fr | Email : service-client@owlsystems.fr

mois à compter de la date de livraison du rapport. Passé ce délai, il est entendu que le Prestataire ne fournit aucune garantie sur la sécurité des systèmes, ces derniers pouvant être affectés par de nouvelles vulnérabilités qui n'étaient pas présentes ou identifiables au moment de l'audit.

Afin de maintenir un niveau de sécurité optimal et de se protéger contre l'évolution des menaces, il est fortement recommandé au Client de procéder à des audits de sécurité réguliers et de mettre en œuvre un suivi continu des mesures de sécurité après l'audit initial.

Le Client est informé que la réalisation d'un audit supplémentaire peut être nécessaire si des changements significatifs sont apportés à l'infrastructure ou aux systèmes après la période de validité de l'audit, ou si des risques nouveaux ou des vulnérabilités non couvertes par l'audit précédent apparaissent.

Section 11 Accès aux locaux du Client (si applicable)

Dans le cadre de l'audit de sécurité, il peut être nécessaire pour le Prestataire d'accéder aux locaux du Client et d'interagir avec les systèmes informatiques du Client, y compris les serveurs, les réseaux et autres infrastructures, afin d'effectuer des tests de sécurité. Le Client reconnaît que ces actions peuvent entraîner des perturbations temporaires, telles que des redémarrages, des interruptions de service ou des déconnexions de serveurs, et accepte de prendre ces risques en connaissance de cause.

Le Client s'engage à fournir un environnement sécurisé pour le Prestataire et à prendre toutes les mesures nécessaires pour protéger les équipements sensibles pendant l'accès aux locaux.

Le Prestataire ne pourra être tenu responsable des conséquences découlant de ces perturbations, y compris mais sans se limiter à :

- La déconnexion imprévue de serveurs ou d'autres systèmes critiques,
- Les pannes temporaires ou les pertes de service,
- Les erreurs techniques résultant de l'intervention dans le cadre de l'audit.

Cependant, le Prestataire s'engage à mener toutes les actions dans le respect des bonnes pratiques de sécurité informatique et de manière non destructive. Toute perturbation causée par des tests effectués dans le cadre de l'audit sera minimisée, mais le Prestataire ne pourra être tenu responsable des dommages résultant de l'exécution des tests, sauf en cas de négligence grave ou de manquement direct aux normes professionnelles.

Le Client s'engage à effectuer une sauvegarde complète de ses systèmes avant l'audit, afin de limiter les risques de perte de données ou d'interruption de services, et accepte de prendre toutes les mesures nécessaires pour se préparer à toute interruption de service potentielle durant l'audit.

Payette Jean (EI) | 10 de la Mare Boutillier – 77166 – Grisy-Suisnes | Tél : 07 56 81 89 12
Siret : 753 004 589 | Site web : www.owlsystems.fr | Email : service-client@owlsystems.fr

Le Client est également responsable de l'application des recommandations du rapport d'audit après l'audit, et toute perturbation résultant d'une non-application des recommandations ne pourra en aucun cas être imputée au Prestataire.

Section 12 Signature et Paraphe

L'acceptation du Contrat peut être formalisée par :

- Signature manuscrite du Devis et des CGV
- Signature électronique via un système sécurisé
- Acceptation explicite par email avec accusé de réception mentionnant le numéro du devis

L'acceptation, quelle que soit sa forme, vaut commande ferme et définitive.

Nom et prénom du Client : **Date** :

Signature manuscrite (à faire précéder de la mention "Lu et approuvé") :

(Signature du Client)

Payette Jean (EI) | 10 de la Mare Boutillier – 77166 – Grisy-Suisnes | Tél : 07 56 81 89 12
Siret : 753 004 589 | Site web : www.owlsystems.fr | Email : service-client@owlsystems.fr

Section 13 Historique des Versions et Annotations

Ce document inclut un espace réservé pour annoter les différentes versions du document. Veuillez noter les modifications effectuées, les dates correspondantes et toute observation pertinente.

Version	Date de mise à jour	Modifications apportées
1.0	12/12/2024	Version initiale
2.0	2025/01/24	Révision exhaustive effectuée dans le but d'améliorer la cohérence, de corriger les doublons et d'assurer l'harmonisation complète des documents

Payette Jean (EI) | 10 de la Mare Boutillier – 77166 – Grisy-Suisnes | Tél : 07 56 81 89 12
Siret : 753 004 589 | Site web : www.owlsystems.fr | Email : service-client@owlsystems.fr