Sommaire (v1)

Contexte et objectifs

Ce rapport présente les résultats d’une évaluation de sécurité effectuée selon le référentiel « Name of the framework » sur le système Y Choisir par [Company]. Les objectifs de ce travail étaient plus précisément de vérifier le niveau de sécurité et de conformité de l’environnement ciblé. Ces tests permettent l’identification de vulnérabilités susceptibles d’être utilisées par un attaquant pour dérober, manipuler les informations, interrompre le service et ainsi dégrader l’image de [Company].

Les tests ont été effectués du XX au XX MMMM YYYY dans les locaux de [Company]. Conformément à la méthodologie d’itrust consulting, tests ont été prévus, et 4 points ont été effectivement testés ( n’entrai[en] t pas dans le champ du test de vulnérabilité et n’étai[en] t pas applicables).

Conformément aux règles d’évaluation applicable aux domaines inclus dans la norme , le niveau d’évaluation est considéré comme Excellent.

Résultats

L’audit a permis d’établir que le niveau de conformité du système dans les domaines considérés inclus dans la norme est Excellent et de formuler les déclarations de non-conformité suivantes :

* non-conformité(s) majeure(s) définie(s) comme une absence totale de documentation ou d’implémentation d’un point de contrôle de la norme conduisant à un dysfonctionnement du système.
* non-conformité(s) mineure(s) définie(s) comme une absence partielle de documentation ou d’implémentation d’un point de contrôle de la norme sans impact actuel et direct sur le fonctionnement du système.
* remarque(s) mettant en exergue une défaillance dans l’implémentation d’un point de contrôle conformément aux bonnes pratiques de sécurité et/ou désignant un point à améliorer par des une ou plusieurs actions précises de sécurité.

L’audit a aussi identifié des points critiques qu’il sera nécessaire de traiter rapidement et de contrôler dans le futur, et dans ce but a formulé les actions à mettre en œuvre (recommandations, actions corrective ou mesures de mitigation) suivantes :

* 0 actions qualifiées par  sur l’échelle de criticité choisie, qui nécessitent une mise en œuvre immédiate pour mitiger un risque qualifié de critique ou une non-conformité majeure.
* 0 actions qualifiées par  sur l’échelle de criticité choisie, qui requièrent une mise en œuvre rapide pour mitiger un risque qualifié d’élevé ou une non-conformité mineure.
* 1 actions, qualifiées par  sur l’échelle de criticité choisie, qui requièrent une mise en oeuvre dédiée pour mitiger un risque qualifié de modéré.
* 0 suggestions qualifiées par  sur l’échelle de criticité choisie et destinées à améliorer l’efficacité ou la sécurité sur des points et qui devraient être directement adressés par le personnel compétent au cours d’un cycle normal d’amélioration.
* 1 notes indiquées par 🗵, pour (à définir)
* 1 notes indiquées par 🗊, nécessitant des investigations pour assurer une évaluation correcte ou augmenter le niveau d’assurance.

Sommaire (v2)

Synopsis

Ce rapport présente les résultats d’une évaluation de sécurité effectuée selon le référentiel "STD Nom" sur le système Y Choisir par [Company]. Les objectifs de ce travail étaient plus précisément de vérifier le niveau de sécurité et de conformité de l’environnement ciblé. Ces tests permettent l’identification de vulnérabilités susceptibles d’être utilisées par un attaquant pour dérober, manipuler les informations, interrompre le service et ainsi dégrader l’image de [Company]..

Les tests ont été effectués du XX au XX MMMM YYYY dans les locaux de [Company]. Conformément à la méthodologie d’itrust consulting, 4 tests ont été prévus, et 4 points ont été effectivement testés (0 n’entrai[en] t pas dans le champ du test de vulnérabilité et 0 n’étai[en] t pas applicables).

Conformément aux règles d’évaluation applicable aux 1 domaines inclus dans la norme "Nom du standard", le niveau d’évaluation est considéré comme Excellent.

Résultats

La première figure ci-dessous donne une vue synthétique des recommandations formulées durant l’audit du système ainsi que des informations additionnelles utiles pour assurer une sécurité pérenne dudit système. La seconde figure offre une vue d’ensemble des tests réalisés classés selon la performance des mesures de sécurité implémentées pour répondre aux exigences des tests. La troisième donne une vue d’ensemble de réussite aux critères mis en œuvre.

Figure 1: Vue synthétique des recommandations, actions correctives et mesures de mitigation

Figure 2: Vue synthétique des résultats aux contrôles



Figure 3: Distribution des résultats des vérifications mises en œuvre

Figure 4: Résumé des résultats relatifs à l’état de résilience

Détails des résultats importants

**Détails de l’évaluation du risque**

Principales vulnérabilités

Au cours de l’audit, itrust consulting a identifié que la majorité des vulnérabilités concernait la gestion du domaine Network avec 1 vulnérabilités.

Impact critique identifié

Parmi les impacts possibles [brèche potentielle de sécurité] identifiés par itrust consulting et inhérents aux vulnérabilités découvertes, les plus importantes sont :

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Niveau | [VUL] | Description |
| IMP. 1 | ▼▼ | [000] | Conséquemment à la vulnérabilité, l’impact potentiel sur le système est… |

**Action de sécurité à mettre en œuvre immédiatement**

Appartenant à la liste des recommandations :

Parmi les recommandations préconisées par itrust consulting, les plus importantes sont :

|  |  |  |
| --- | --- | --- |
| ID | Niveau | Description |
| REC. 1 |  | Faire …(mode infinitif) |
| REC. 4 |  | Faire …(mode infinitif) |

Appartenant à la liste des mesures de mitigation :

Parmi les mesures préconisées par itrust consulting, les plus importantes sont :

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Niveau | [VUL┆IMP] | Description |
| MIT. 1 |  | [000┆000] | Faire …(mode infinitif) |

Appartenant à la liste des actions :

Parmi les actions correctives décidées conjointement avec le client, les actions les plus importantes sont :

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Niveau | Date limite | Description |
| AC. 3 |  | 07/2014 | Faire…(mode infinitif) |
| AC. 3 |  | 07/2014 | Faire…(mode infinitif) |

**Investigation à réaliser ultérieurement**

Les points suivants nécessitent d’être contrôlés plus avant durant un audit interne ou externe ultérieur :

Appartenant à la liste des recommandations :

|  |  |  |
| --- | --- | --- |
| ID | Échelle | Description |
| REC 12. |  | Faire…(mode infinitif) |

Appartenant à la liste des actions :

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Échelle | Deadline | Description |
| AC 13. |  | 07/2014 | Faire…(mode infinitif) |

Points positifs de l’implémentation du système

Concernant la résilience tant au niveau du design ou de l’implémentation de la sécurité pour le système ciblé, itrust consulting a identifié les points positifs suivants :

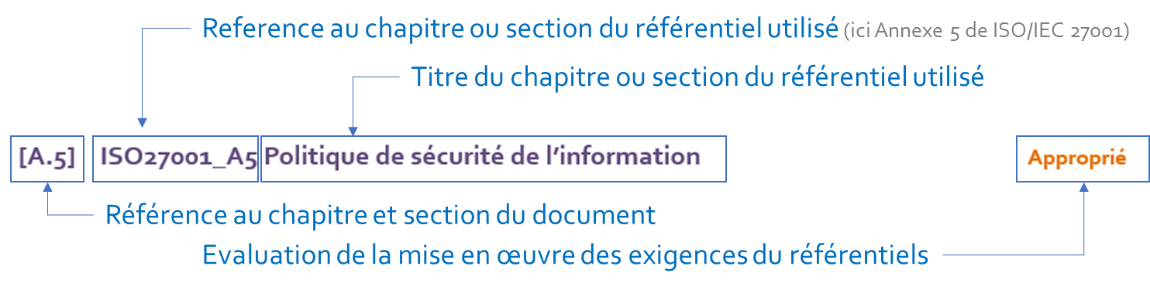
|  |  |  |
| --- | --- | --- |
| ID | Niveau | Description |
| RP. 1 |  | Le système présente…. (present tense) |
| RP. 2 |  | Le système présente… (indicatif présent) |

## Convention éditoriale utilisée dans ce rapport

Ce chapitre décrit la convention éditoriale choisie en particulier les échelles utilisées pour évaluer le niveau de sécurité du système cible ainsi que les actions de sécurité qui pourraient être mises en œuvre pour améliorer ou maintenir ce niveau.

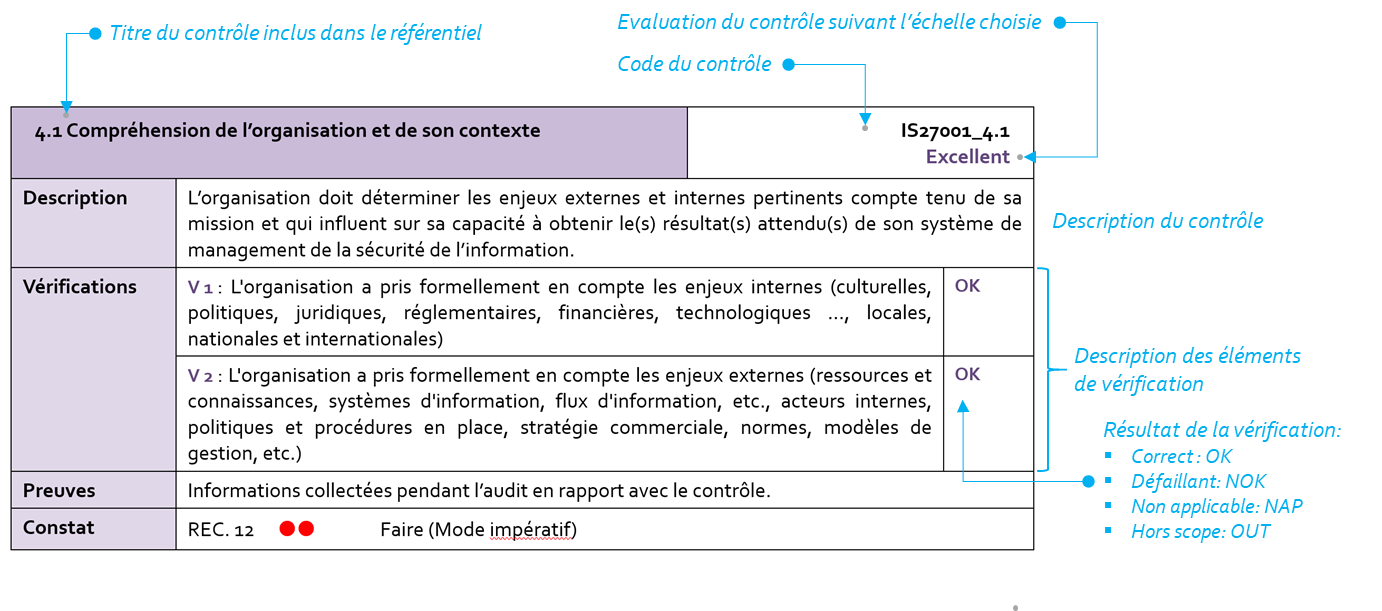
### Titre

Afin d’indiquer les références aux normes et guides de sécurité utilisés durant cet audit, le rapport adopte la convention suivante pour le titrage.



### Convention des tableaux de vérification

L’exemple suivant explique comment lire les différents types de tables utilisables dans le rapport.



Note : Si des éléments de vérifications contenues dans un tableau font référence à un point plus spécifique contenu dans un autre tableau, le rapport n’évaluera cet élément qu’une fois pour éviter de répéter la même non-conformité ou la même action corrective à plusieurs endroits du document.

Pour évaluer la mise en œuvre de chaque bonne pratique à atteindre ou contrôler les mesures de sécurité considérées, on déterminera la conformité ainsi que le niveau de maturité atteint dans l’implémentation de la sécurité. Le tableau ci-dessous donne les critères de détermination du taux d’implémentation et de maturité :

|  |  |  |
| --- | --- | --- |
| Niveau de Maturité | CMMI Model | Description |
| Niveau 1 | Initial | Processus / Système imprévisible, mal contrôlé et réactif. |
| Niveau 2 | Géré | Processus / Système mis en œuvre et géré par le professionnalisme (proactif). |
| Niveau 3 | Défini | Processus / Système défini et mis en œuvre selon une approche standardisée. |
| Niveau 4 | Contrôlé | Processus / Système régulièrement contrôlé et évalué. |
| Niveau 5 | Optimisé | Processus / Système régulièrement revu selon une approche de cycle d'amélioration. |

Table 1: Critère d’implémentation et de maturité

### Interprétation du rapport

Le rapport utilise différentes échelles pour évaluer soit la conformité du système aux exigences de sécurité, soit le niveau de criticité des éléments identifiés, soit les actions de sécurité à entreprendre, soit encore le niveau général des tests effectués au cours de l’audit. Les tableaux ci-dessous décrivent les échelles choisies et donnent une description brève de chaque niveau.

#### Définition du niveau de non-conformité

L’audit doit fournir une évaluation de la conformité du système conformément au référentiel Nom du référentiel et aux bonnes pratiques de sécurité pour chaque domaine considéré de manière à produire une vision claire du niveau de sécurité de l’organisation ou du système. La non-conformité d’un domaine est évaluée soit comme majeure, soit comme mineure en fonction de sa gravité. Des remarques peuvent être formulées soit pour corriger ou pour améliorer un point du domaine considéré.

|  |  |
| --- | --- |
| Niveau de non-conformité | Description |
| Non-conformité majeure | Non-respect d’une exigence qui a une incidence sur la capacité d’atteindre les résultats escomptés. Note : Une non-conformité peut être qualifiée de majeure dans les circonstances suivantes :   * s’il existe un doute sérieux que des mesures efficaces aient été mises en œuvre, ou que le produit ou le service atteigne les exigences spécifiées ; * un certain nombre de non-conformités mineures associées à la même exigence ou au même problème laissent à penser que la défaillance est d’ordre systémique et qu’il constitue de ce fait une non-conformité majeure. |
| Non-conformité mineure | Non-respect d’une exigence qui n’affecte pas cependant la capacité d’atteindre les résultats escomptés. |
| Remarque | Observation à prendre en compte dans le processus d’amélioration continue ou le processus de traitement des risques. |

#### Échelle d’évaluation des critères mis œuvre ou des vulnérabilités

L’échelle utilisée pour évaluer le résultat de la vérification d’un critère de sécurité est graduée en plusieurs niveaux d’évaluation :

|  |  |
| --- | --- |
| Échelle | Description |
| Non évalué | L’évaluateur ne dispose pas d’éléments suffisants pour conclure sur ce point. |
| Bien implémenté | Les critères sont bien remplis à l’aide de mesures qui dépassent l’état de l’art et qui offrent plus de sécurité que des implémentations standards. |
| Approprié | Les critères sont correctement mis en œuvre compte tenu l’état de l’art. |
| Satisfaisant | Les critères sont mis en œuvre, mais compte tenu l’état de l’art, les risques sont maitrisés, mais des points d’amélioration ont été identifiés. |
| À améliorer | Les critères sont remplis a minima, mais la sécurité de l’ensemble présente toujours des risques acceptables mais inutiles, car la prise en compte de l’état de l’art aurait permis de les réduire. |
| En partie satisfait | Les critères sont en général remplis sauf pour un ou plusieurs éléments ponctuels qui présentent des risques limités. |
| Non satisfait | Les critères sont en aucune façon remplis : absence de mesures de sécurité nécessaires constituant une vulnérabilité patente pour la sécurité des systèmes. |
| Non testé | Les critères n’ont pas été contrôlées sur le système cible. |
| Non applicable | Les critères ne sont pas applicables au système cible. |
| Hors périmètre | Impossibilité d’évaluer le contrôle du fait de la définition ou de la nature du système cible. |

#### Échelle d’évaluation des domaines

L’échelle utilisée pour évaluer un domaine spécifique de la sécurité est identique à celle utilisée pour évaluer un critère de sécurité ou une vulnérabilité (voir plus haut) mais elle portera sur l’ensemble des critères ou l’ensemble des vulnérabilités afférents à ce domaine de sécurité.

#### Évaluation automatique des contrôles, domaines de sécurité et de la sécurité globale

Même si l’évaluation des différentes éléments (contrôle, domaine de sécurité ou sécurité Générale) est laissée à la seule appréciation de l’auditeur, il peut aussi effectuer ces évaluations de manière automatique en appliquant les matrices de calcul correspondantes décrites ci-dessous.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | L’implémentation d’un contrôle est considérée comme : | | | | | | |
|  | Non évalué | Bien implémenté | Approprié | Satisfaisant | À améliorer | En partie satisfait | Non satisfait |
| Premier niveau d’évaluation : si la somme des non-conformités et des non-conformités supérieurs est supérieure ou égale : | | | | | | | |
| Majeure | Désactivé |  |  |  |  |  | 01 |
| Mineure | Désactivé |  |  | 01 | 02 | 03 | 05 |
| Second niveau d’évaluation : si la somme des recommandations pour un certain niveau et des niveaux supérieurs est supérieure ou égale à : | | | | | | | |
|  | Désactivé |  |  |  |  |  | 001 |
|  | Désactivé |  |  |  | 001 | 002 | 005 |
|  | Désactivé |  |  | 001 | 002 | 005 | 010 |
|  | Désactivé |  | 002 | 003 | 005 | 010 | 020 |
| Troisième niveau d’évaluation : si son implémentation est évaluée au niveau de résilience suivant : | | | | | | | |
|  | Désactivé |  |  |  |  |  |  |
|  | Désactivé |  |  |  |  |  |  |
|  | Désactivé | 1 |  |  |  |  |  |
| Quatrième niveau d’évaluation : si la somme de points supplémentaires à contrôler ou de points spécifiques est supérieure ou égale à : | | | | | | | |
| À vérifier  | Désactivé |  |  |  |  |  |  |
| Spécifique 🗵 | Désactivé | 001 |  |  |  | 015 | 020 |

Table 2: Matrice d’évaluation automatique des contrôles

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Un domaine est considéré comme | | | | | | |
|  | Bien implémenté | Approprié | Satisfaisant | À améliorer | En partie satisfait | Non satisfait |  |
| *Si l’évaluation des résultats en % des contrôles du domaine selon les catégories respectent les règles de répartitions suivantes :* | | | | | | | |
| Non évalué | Désactivé | Désactivé | Désactivé | Désactivé | Désactivé | Désactivé | 🡅≥  Règle 1 |
| Bien implémenté | 75 % | 0 % | 0 % | 0 % | 0 % | 0 % |
| Approprié | 25 % | 75 % | 0 % | 0 % | 0 % | 0 % |
| Satisfaisant | 0 % | 25 % | 75 % | 0 % | 0 % | 0 % |
| À améliorer | 0 % | 0 % | 25 % | 75 % | 0 % | 0 % |
| En partie satisfait | 0 % | 0 % | 0 % | 25 % | 75 % | 25 % | 🡇≤  Règle 2 |
| Non satisfait | 0 % | 0 % | 0 % | 0 % | 25 % | 75 % |

Table 3 : Matrice d’évaluation automatique des domaines

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Le système cible dans sa globalité est considéré comme | | | | | | |
|  | Bien implémenté | Approprié | Satisfaisant | À améliorer | En partie satisfait | Non satisfait |  |
| Si l’évaluation des résultats en % des domaines selon les catégories respectent les règles de répartitions suivantes : | | | | | | | |
| Bien implémenté | 75 % | 0 % | 0 % | 0 % | 0 % | 0 % | 🡅≥  Règle 1 |
| Approprié | 25 % | 75 % | 0 % | 0 % | 0 % | 0 % |
| Satisfaisant | 0 % | 25 % | 75 % | 0 % | 0 % | 0 % |
| À améliorer | 0 % | 0 % | 25 % | 75 % | 0 % | 0 % |
| En partie satisfait | 0 % | 0 % | 0 % | 25 % | 75 % | 10 % | 🡇≤  Règle 2 |
| Non satisfait | 0 % | 0 % | 0 % | 0 % | 25 % | 90 % |

Table 4 : Matrice d’évaluation globale automatique du système cible

#### Échelle de criticité des actions de sécurité conseillées

La table ci-dessous décrit l’échelle de criticité utilisée pour évaluer l’importance de l’action de sécurité conseillée (recommandations ou actions correctives) dans le rapport.

|  |  |  |
| --- | --- | --- |
| Échelle | Étiquette | Description |
|  | Critique | Situation de risque inacceptable ou de non-conformité majeure qui requière une action immédiate (typiquement le jour de la découverte). |
|  | Urgent | Situation de risque ou de non-conformité, inacceptable d’un point de vue sécurité, contractuel ou juridique, mais qui pourrait être accepté temporairement par le management en fonction d’autres considérations. |
|  | Important | Situation de risque acceptable, mais inutile, ou absence de mesures recommandées selon l’état de l’art. |
|  | Utile | Situation de risque faible ou de manque d’efficacité, avec des suggestions d’amélioration connues. |
|  | Spécifique | Qualification à déterminer (spécifique) |
|  | À contrôler | Nécessité de réaliser des investigations plus spécifiques que ceux prévues dans le présent projet. |

#### Échelle de résilience

Si un contrôle ou un test révèle que la sécurité du système présente de bien meilleures caractéristiques que celles attendues dans ce genre de système, selon les bonnes pratiques de la sécurité, l’auditeur pourra utiliser l’échelle suivante pour souligner la résilience du système cible.

|  |  |
| --- | --- |
| Échelle | Description |
|  | La mesure de sécurité mise en place est fondée sur une solution innovante et durable capable d’assurer réellement la sécurité en profondeur. |
|  | La mesure de sécurité est fondée sur la solution la plus sûre connue à ce jour. |
|  | La mesure de sécurité choisie est meilleure que celle généralement préconisée par les bonnes pratiques dans ce genre de situation. |

#### Modèle typologique d’identification des vulnérabilités

Les vulnérabilités identifiées durant l’audit du système sont évaluées selon le modèle suivant :

|  |  |  |
| --- | --- | --- |
| Symbole | Nom | Description |
| **🏭** | Infrastructure | Vulnérabilité de l’infrastructure comme absence de système anti-incendie, de redondance du câblage, etc… |
| **🖧** | Réseau | Vulnérabilité des réseaux de communication et des équipements afférents comme pare-feu, switch, routeur, etc… |
| **💻** | Hardware | Vulnérabilité du hardware mis en œuvre tel que des erreurs de dimensionnement de l’équipement, équipement non sécurisé, etc… |
| **🗗** | Software | Vulnérabilité des logiciels mis en œuvre généralement en fonction de la connaissance contenue dans les bases de données de vulnérabilité. |
| **🛠** | Déploiement | Vulnérabilité due à des erreurs d’implémentation, de configuration ou de maintenance. |
| **👁** | Management | Vulnérabilité due à la mauvaise gestion de la sécurité : manque de personnel qualifié, manque de temps pour a gestion de la sécurité… |
| **🚹** | Humaine | Vulnérabilité directe ou indirecte relative au personnel mettant en œuvre le système ou sa sécurité tels que défaut de sensibilisation à la sécurité ou de formation. |

#### Échelle d’impact

Compte tenu des vulnérabilités découvertes, le présent rapport établit les impacts potentiels en cas d’exploitation de la vulnérabilité. L’échelle d’impact suivante permet de mesurer sa criticité de l’impact :

|  |  |  |
| --- | --- | --- |
| Symbole | Nom | Description |
| **⯇⯇⯇⯇** | Critique | En cas d’exploitation de la vulnérabilité, le système ou le processus supporté par l’actif vulnérable pourrait être :  totalement détruit *— ex. destruction de l’équipement dû au feu.*  Inopérant pendant un temps très long *— ex. chiffrement malicieux d’un disque dur.* |
| **⯇⯇⯇** | Élevé | En cas d’exploitation de la vulnérabilité, le système ou le processus supporté par l’actif vulnérable pourrait être compromis (perte de contrôle, des propriétés de confidentialité ou d’intégrité du système entier). *— ex. blocage des transmissions* |
| **⯇⯇** | Modéré | En cas d’exploitation de la vulnérabilité, le système ou le processus supporté par l’actif vulnérable pourrait être altéré sans pour autant qu’il y ait une perte de contrôle ou une atteinte aux propriétés de confidentialité et d’intégrité du système entier.  *— ex. réduction de la vitesse de calcul des processus.* |
| **⯇** | Faible | En cas d’exploitation de la vulnérabilité, le système ou le processus supporté par l’actif vulnérable demeure opérationnel, mais la protection fournie par l’actif est maintenant inopérante et le système entier voit sa vulnérabilité augmenter.  *— Ex. mauvaise configuration d’un pare-feu.* |

This line includes an essential bookmark E\_F: do not remove

# Conclusion

Après X jours d’audit du système ciblé, itrust consulting conclu que Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum

Les tableaux ci-dessous donnent un résumé concis des résultats des tests et contrôles effectués, du niveau de sécurité atteint par le système cible compte tenu de la demande du maître d’ouvrage en termes de focus, de granularité ou de recherche de l’audit.

## Évaluation des domaines de sécurité

La table ci-dessous donne un résumé de l’évaluation des domaines considérés durant l’audit ainsi qu’une évaluation globale de la conformité du système ciblé.

|  |  |  |
| --- | --- | --- |
| Évaluation des domaines de sécurité considérés | | Total/Type |
| Bien implémenté | | 0 |
| Approprié | | 0 |
| Satisfaisant | | 0 |
| À améliorer | | 0 |
| En partie satisfait | | 0 |
| Non satisfait | | 0 |
| Non applicable | | 0 |
| Hors périmètre | | 0 |
| Résultat global pour le système cible | En partie satisfait | |

Table 5 : Résultat de l’évaluation des domaines de sécurité pour le système cible

En conclusion, la sécurité globale du système cible évalué selon **1** des **1** domaines inclus dans la norme/guide … utilisée est considérée comme étant En partie satisfait.

Détail de l’évaluation[[1]](#footnote-1)

| Référence | Titre | Rating |
| --- | --- | --- |
| [\*.\*] | Acronyme et titre du domaine | Rating |

Table 6: Résultats par domaine de sécurité

## Évaluation de la conformité

La conclusion de l’audit réalisé sur le système cible a conduit itrust consulting à identifier des cas de non-conformité et à émettre aussi des remarques sur la mise en œuvre de la .

Les tableaux ci-dessous donnent un aperçu synthétique des cas de non-conformité et des remarques formelles figurant dans ce document.

|  |  |
| --- | --- |
| Type de non-conformité | Total/Type |
| Majeure manque total de documentation ou d’implémentation | 1 |
| Mineure manque partiel de documentation ou d’implémentation | 0 |
| Remarque point à corriger ou à améliorer | 0 |
| Total | 1 |

Table 7 : Résumé des points de l’évaluation de la conformité

La liste ci-dessous donne le détail des non-conformités trouvées au cours de l’audit :

| ID | Évaluation | Réf. | Description |
| --- | --- | --- | --- |
| NC1. | Minor | 9.9.9 |  |

Table 8: Liste des non-conformités

## Résumé des vulnérabilités identifiées

Le tableau suivant donne une vue d’ensemble des types de vulnérabilités découvertes durant l’audit sur le système ciblé.

|  |  |
| --- | --- |
| Type de vulnérabilité | Total/Type |
| 🏭 Infrastructure | 0 |
| 🖧 Network | 1 |
| 💻 Hardware | 0 |
| 🗗 Software | 0 |
| 🛠 Mise en œuvre | 0 |
| 👁 Management | 0 |
| 🚹 Humain | 0 |
| Total | 1 |

Table 8: Résumé du nombre de vulnérabilités identifiées par type

La liste suivante donne le détail des vulnérabilités découvertes durant l’audit effectué sur le système déployé par :

| ID | Type | Description |
| --- | --- | --- |
| VU1. |  | Le système présente la vulnérabilité suivante : … |

Table 10: Liste des vulnérabilités par type

## Résumé des impacts potentiels

En lien avec l’évaluation de la vulnérabilité du système, l’audit a évalué selon criticité l’impact probable sur le système en cas d’exploitation de chacune des vulnérabilités découvertes.

|  |  |
| --- | --- |
| Criticité des impacts | Total/Type |
| ⯇⯇⯇⯇ Critique | 2 |
| ⯇⯇⯇ Elevé | 0 |
| ⯇⯇ Modéré | 0 |
| ⯇ Faible | 0 |
| Total | 2 |

Table 9 : Résumé des impacts potentiels

La liste suivante donne le détail des impacts potentiels en cas d’exploitation des vulnérabilités découvertes :

|  |  |  |
| --- | --- | --- |
| ID | Rating | Description |
| IM1. |  | Consequently to the vulnerability, the potential impact is… |

Table 12: Liste des impacts potentiels

## Résumé des actions correctives à mettre en œuvre

Le résumé ci-dessous donne une vue d’ensemble des actions correctives préconisées et acceptées par le maître d’ouvrage pour assurer ou améliorer le niveau de sécurité du système cible et pour retrouver le niveau de conformité requis.

|  |  |
| --- | --- |
| Niveau de criticité des actions à mettre en œuvre | Total/Type |
|  Action immédiate requise | 1 |
|  Action rapide requise | 1 |
|  Action dédiée requise | 1 |
|  Notes utiles pour améliorer la sécurité | 0 |
| 🗵 Niveau à définir | 0 |
| 🗊 Investigation ou contrôle additionnels requis | 0 |
| Total | 3 |

Table 10: Résumé des actions correctives

La liste ci-dessous donne le détail de toutes actions correctives à mettre en œuvre qui ont été identifiées durant l’audit du système déployé par :

| Réf. | Évaluation | Délais | Description |
| --- | --- | --- | --- |
| AC. 1 |  | 07/2014 | Faire…. (Mode infinitif) |

Table 14: List of corrective actions

## Résumé des recommandations identifiées

Le résumé ci-dessous donne une vue d’ensemble des recommandations faites par l’auditeur pour assurer ou améliorer le niveau de sécurité du système cible et pour retrouver le niveau de conformité requis si nécessaire.

|  |  |
| --- | --- |
| Niveau des recommandations | Total/Type |
|  Action immédiate requise | 1 |
|  Action rapide requise | 0 |
|  Action dédiée requise | 0 |
|  Notes utiles pour améliorer la sécurité | 1 |
| 🗵 Niveau à déterminer | 1 |
| 🗊 Investigation ou contrôle additionnels requis | 1 |
| Total | 4 |

Table 11 : Résumé des recommandations identifiées

La liste ci-dessous donne le détail de toutes les recommandations préconisées durant la revue de sécurité du système déployé par :

| Réf. | Évaluation | Description |
| --- | --- | --- |
| REC. 1 |  | Faire (Mode infinitive) |

Table 16: Liste des recommandations

## Résilience du système

Au cours de l’audit, itrust consulting a identifié des points positifs dans le design, l’implémentation ou la maintenance du système ciblé. Parmi ces points positifs, les points suivants ont été considérés comme le fondement de la résilience dudit système :

| ID | Évaluation |  |
| --- | --- | --- |
| RP. 1 |  | Le système présente… |

Table 17: Liste des points de résilience du système

## Résumé des résultats par critères de sécurité

Le tableau ci-dessous donne une vue globale du résultat des tests ou contrôles effectués selon l’échelle précédemment décrite dans le présent document.

|  |  |
| --- | --- |
| Évaluation pour les contrôles effectués sur le système cible | Total/Type |
| Non évalué | 5 |
| Bien implémenté | 0 |
| Approprié | 0 |
| Satisfaisant | 0 |
| À améliorer | 0 |
| En partie satisfait | 0 |
| Non satisfait | 0 |
| Non testé | 0 |
| Non applicable | 0 |
| Hors périmètre | 0 |
| Total | 5 |

Table 12 : Résumé des résultats par critère

La liste suivante donne le détail des contrôles effectués avec leur évaluation.

| Référence | Titre | Rating |
| --- | --- | --- |
| REF9999\_0.0.0 | 0. Convention éditoriale | Satisfaisant |

Table 19: Liste des résultats par critère de sécurité

## Résultats des vérifications par contrôle

Le tableau ci-dessous donne un aperçu global des résultats des vérifications effectuées pour chaque critère de sécurité évalué.

|  |  |
| --- | --- |
| Résultat des vérifications | Total/Type |
| OK (Vérification satisfaite) | **1** |
| NOK (Vérification non satisfaite) | 3 |
| OUT (Vérification hors périmètre) | 75 |
| NAP (Vérification non applicable)) | 5 |
| Total |  |

Table 20: Résumé des résultats des vérifications

La table ci-dessous donne un aperçu des résultats des vérifications par critère et par domaine de sécurité.

| Référence | Titre | OK | NOK | OUT | NAP | Évaluation |
| --- | --- | --- | --- | --- | --- | --- |
| [2] | Premier domaine | 1 | 2 | 3 |  | En partie satisfait |
| IS27001\_A.11.1 | A.11.1 Sécurité de l’environnement physique |  |  |  |  | En partie satisfait |

Table 21: Distribution des résultats des vérifications par critères et par domaine

## Résumé des mesures de mitigation

Le tableau ci-dessous donne un aperçu des mesures de mitigation identifiées au cours de l'audit en fonction de leur criticité.

|  |  |
| --- | --- |
| Niveau de criticité de la mitigation | Total/Type |
|  Action immédiate requise | **1** |
|  Action rapide requise | **1** |
|  Action dédiée requise | **0** |
|  Possible amélioration de la sécurité | **0** |
| Total | 2 |

Table 7: Summary of identified mitigation measures

La table ci-dessous donne la liste des mesures de sécurité identifiées pour mitiger des vulnérabilité sur le système cible :

|  |  |  |  |
| --- | --- | --- | --- |
| Ref | Niveau | [VUL┆IMP] | Description |
| MIT. 1 |  | [000┆000] | To mitigate the identified vulnerability and avoid impact, do ... (imperative tense) |
| MIT. 2 |  | [000┆000] | To mitigate the identified vulnerability and avoid relative impact, do … (imperative tense) |

Table 8: List of mitigation measures

## Résumé des résultats relatifs à l’état de résilience

La table ci-dessous fournit un résumé des résultats relatifs à l’état de résilience du système tel qu’établi lors de l’audit selon l’échelle définie dans ce même tableau :

|  |  |  |
| --- | --- | --- |
| Résumé des résultats | | Total/Type |
|  | Description du niveau |  |
| Total | |  |

Table 24: Liste des résultats relatifs à l’état de résilience

La table ci-dessous liste l’ensemble des résultats relatifs à l’état de résilience du système tel qu’établi lors de l’audit :

|  |  |  |
| --- | --- | --- |
| Ref | Niveau | Description |
| CUST. 1 |  | Description des résultats spécifiques |

Table 25: Liste des résultats relatifs à l’état de résilience

## Évaluation globale de la sécurité du système testé

Le tableau (panel de sécurité) ci-dessous donne un panel de synthèse du niveau de sécurité du système testé selon l'évaluation des vulnérabilités. De plus, il fournit la liste des recommandations identifiées en fonction de l'impact potentiel d'une attaque visant une vulnérabilité spécifique..

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID VUL | Type | Vulnérabilité système | ID IMP | Niv. | Impact si exploitation vulnérabilité | ID MIT | Niv. | Recommandation/Mitigation |
| 001 |  | Vulnérabilité | **001** | ▼▼▼▼ | Impact potentiel | **001** |  | Mitigation |

Table 26: Security panel

This line includes an essential bookmark C13 : do not remove

1. Le nombre du chapitre entre crochet permet de montrer si l’évaluation s’est focalisée sur un sous-domaine de la norme ou du guide utilisé afin d‘évaluer un point spécifique de contrôle. [↑](#footnote-ref-1)