TRAVAIL PERSONNEL

Audit – Approche par Vecteurs

Module 1 – Stratégie de la Sécurité des Systèmes d'Information

DAS – Gouvernance de la Sécurité des Systèmes d'Information (MAS MSSI)

Renie ALMIRAL

18 octobre 2023

Table des matières

1. Contexte

Dans le cadre du premier travail personnel du DAS GSSI, l'objectif est d'effectuer un audit sur la gouvernance des systèmes d'information (SI) au sein d'une entreprise. Pour mener à bien cet audit, le choix s'est porté sur l'entreprise VIRTUIX, une entreprise fictive. L'audit est basé sur l'approche par vecteurs, accompagné d'une évaluation du niveau de maturité en utilisant le modèle d'intégration de la capacité et de la maturité[1].

VIRTUIX est une entreprise suisse fondée par des passionnés de cybersécurité. Ils ont développé SimulIT, un logiciel de simulation de cybersécurité en réalité virtuelle (VR) pour une formation interactive et réaliste. Compte tenu de la réussite de l'application, la société se développe rapidement. Toutefois, elle rencontre des obstacles en matière de la gestion de son système informatique et de sécurité. Les ingénieurs systèmes effectuent les tâches et les projets sur demande ou en réponse à un incident. Parallèlement, ils sont sollicités pour fournir un support technique. La durée de ces interventions téléphoniques varie en fonction de la complexité des problèmes des utilisateur finaux, entraînant parfois des retards dans l'exécution des tâches des projets à faire. Il existe un minimum de documentation établi telle que la topologie réseau physique et logique, la liste d'appareils et mots de passe, quelques configurations, des politiques et des procédures. À l'heure actuelle, le plan d'évolution du système d'information manque de clarté en raison d'un manque de gouvernance. Le Directeur Général se rend compte que la croissance de l'entreprise prend de l'ampleur et nécessite un système informatique mieux adapté aux besoins de ses employés ainsi que la capacité à maintenir la prestation de services de qualité à ses clients.

Ce document est divisé en quatre parties : *Présentation de l'entreprise*, *Méthodologie d'évaluation et les niveaux de maturité*, *Analyse par vecteur* et *Conclusion*. La première partie est dédiée à la présentation de l'entreprise VIRTUIX. Quelques éléments essentiels seront abordés tels que ses services principaux, son public cible ainsi que sa structure de gestion et sa hiérarchie. La deuxième partie sert à définir les cinq niveaux de maturité pour chaque vecteur. Pour ce travail, il existe 12 vecteurs à analyser. Il est important de noter que les vecteurs ont été modifiés afin de s'adapter à l'entreprise. Puis, l'analyse par vecteur consiste à faire un état des lieux, d'analyser la situation actuelle pour chaque vecteur et de les évaluer selon les niveaux de maturité détaillés à la partie précédente. Finalement, la dernière partie a pour objectif d'analyser les résultats des niveaux de maturité de chaque vecteur, en créant un graphe de scoring. Le but est de proposer des pistes d'amélioration et de mettre en évidence les forces et les faiblesses de l'entreprise dans la gouvernance de son système d'information.

[1] *Capability Maturity Model Integration ou CMMI*

2. Présentation de l’entreprise - VIRTUIX

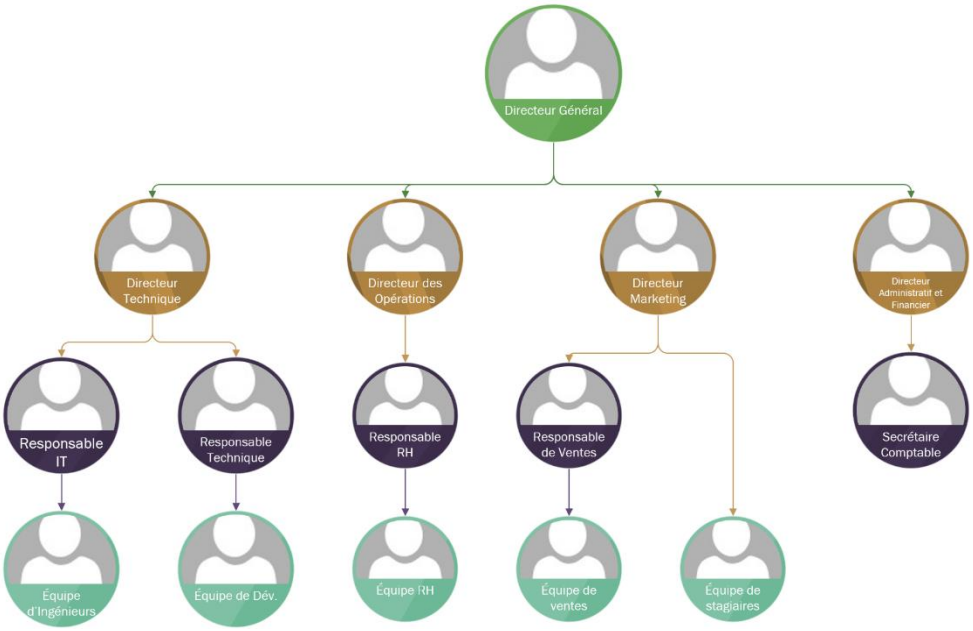
L'entreprise VIRTUIX a été fondée sur l'idée de l'un de ses membres fondateurs qui est passionné par la cybersécurité. Ils ont développé le produit SimulIT, un logiciel de simulation de situations liées à la cybersécurité en utilisant la réalité virtuelle (VR) pour rendre l'apprentissage interactif et réaliste.

L’application SimulIT offre divers scénarii basés sur des situations réelles en cybersécurité, notamment la découverte de fichiers infectés, des fuites de données, ou des attaques sur des plateformes web. L'objectif est de mettre l'utilisateur en situation, non seulement sur le plan technique, mais aussi en impliquant différents acteurs internes et externes à l'entreprise. L'entreprise propose deux modèles d'approvisionnement, notamment sous forme de standalone avec une durée de support de deux ans, ou sous forme de SaaS avec un abonnement annuel par utilisateur.

VIRTUIX cible principalement les entreprises Suisses cherchant à former leurs employés à des scénarios concrets, en se positionnant en tant que produit business-to-business (B2B). Le produit s'adresse à des entreprises de toutes tailles, mais avec une préférence pour les moyennes et grandes entreprises. Il nécessite un investissement significatif dans la formation en cybersécurité, ce qui le rend moins adapté aux entreprises à budget limité. L'entreprise propose également des forfaits spéciaux pour les start-ups actives dans ce domaine.

L’entreprise est en plein développement et compte moins de 50 collaborateurs. En ce qui concerne le département informatique, il n’existe que deux ingénieurs systèmes en charge de la gestion des systèmes informatiques de l’entreprise, sous la supervision du Responsable IT. De plus, ils sont chargés de fournir un support technique, tant en interne qu’auprès des clients. Aucune équipe de sécurité informatique n’a été mise en place.

2.1 Management et hiérarchie



3. Méthodologie d'évaluation et les niveaux de maturités

VECTEUR 1 – STRATEGIE SI	La stratégie SI devrait s'aligner sur les objectifs stratégiques de l'entreprise en élaborant une planification et une feuille de route. De plus, une gestion de portefeuille permet de prioriser la création de valeur et garantir l'allocation adéquate de ressources. La stratégie SI est communiquée efficacement à l'ensemble de l'organisation.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Aucune stratégie SI. L'entreprise ne perçoit pas l'importance d'aligner son SI sur les objectifs de l'entreprise. Les décisions sont prises de façon réactive ou au cas par cas et sans vision stratégique pour son SI.	Bien qu'une stratégie SI existe, elle n'est pas alignée sur la stratégie de l'entreprise. Les décisions sont prises en se basant sur les besoins immédiats sans prise en compte d'une vision à long terme. Manque de coordination entre les projets SI et les priorités de l'entreprise.	Une stratégie SI établie mais partiellement alignée sur les objectifs de l'entreprise. L'entreprise reconnaît l'importance de l'alignement des SI mais des lacunes persistent en matière de l'alignement stratégique.	La stratégie SI est clairement définie et alignée sur la stratégie de l'entreprise. Les décisions sont prises de manière réfléchie en prenant compte à la fois les besoins à court et à long terme.	La stratégie SI est entièrement alignée sur la stratégie de l'entreprise. Il existe des plans à long terme pour le développement des SI accompagnés d'une vision claire. Les SI sont perçus comme un atout stratégique pour l'entreprise.
VECTEUR 2 – POLITIQUE ET PROCEDURES SI	Les politiques et les procédures SI favorisent la conformité réglementaire, la sécurité des données et une gestion efficace des systèmes d'information au sein de l'entreprise. Il est important de formaliser ces directives, de les communiquer à l'ensemble des collaborateurs et de mettre en place un suivi pour s'assurer de leur application.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Absence de politiques et procédures en matière de SI. Manque de directives pour la gestion, la sécurité et la conformité SI. Les actions sont prises de manière réactive sans structure ni planification.	Des politiques et procédures existent mais ne sont pas officiellement documentées. Les décisions sont prises de manière ad hoc.	Documentation de certains politiques et procédures mais leur application est incohérente. Les collaborateurs ne sont pas au courant de ces documents ou ne peuvent pas les suivre de manière cohérente. Pas de suivi, ni de révision des documents.	Les politiques et procédures sont documentées et communiquées aux collaborateurs. Il existe une culture de conformité et de respect des directives établies.	Les politiques et les procédures sont régulièrement révisées et améliorées en réponse aux évolutions technologiques et aux besoins de l'entreprise. La conformité, la sécurité et l'efficacité du SI sont constamment renforcées.
VECTEUR 3 – GESTION DE RESSOURCES SI	La gestion des ressources assure une allocation efficace des ressources humaines, financières et technologique, alignées sur les objectifs de l'entreprise. Il est important de mettre en place des processus de gestion des ressources SI, de planifier à court et à long terme et de veiller à l'alignement sur les objectifs de l'entreprise. Une gestion efficiente permet d'optimiser les investissements, de maximiser la productivité et de contribuer de manière significative aux objectifs de l'entreprise.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Les ressources disponibles sont sous-utilisées ou mal gérées. Manque de coordination et planification des ressources.	Gestion de ressources insuffisante ou désorganisée. Les ressources sont utilisées de manière réactive, sans planification à long terme ni l'alignement sur les objectifs de l'entreprise.	Reconnaissance de la nécessité d'amélioration de la gestion des ressources SI mais manque de coordination et de cohérence.	Les ressources sont correctement allouées et gérées selon les besoins grâce à la mise en place des processus de la gestion des ressources SI. Une planification à court et à long terme favorisant l'efficacité et l'alignement stratégique.	Les ressources sont optimisées pour atteindre les objectifs stratégiques tout en minimisant les coûts inutiles. La gestion des ressources SI fait partie de la culture de l'entreprise.
VECTEUR 4 – GESTION DES RISQUES SI	La gestion des risques consiste à identifier, évaluer et gérer les menaces potentielles aux SI de l'entreprise.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Les risques ne sont pas identifiés ou mal gérés. Peu ou pas de processus mis en place.	Reconnaissance de l'importance de la gestion des risques liés aux SI mais les initiatives sont irrégulières et basées sur des réponses réactives. Les risques ne sont pas évalués et les actions correctives sont prises au cas par cas.	Des processus de gestion des risques sont établis mais pas encore systématisés. La gestion des risques est concentrée seulement sur certains domaines. Manque de communication des risques au sein de l'entreprise.	La gestion des risques est bien établie grâce au processus. Les risques sont évalués de manière systématique et une communication adéquate au sein de l'entreprise existe.	La gestion des risques est intégrée dans toutes les décisions et activités liées aux SI. Les mesures préventives, correctives et mitigation sont mises en place. Des plans de continuité d'activité et de reprise des activités sont établis.
VECTEUR 5 – SECURITÉ DES DONNÉES SI	La sécurité des données SI se concentre à la protection des informations sensibles et critiques de l'entreprise, la sensibilisation des collaborateurs, la veille technologique ainsi que la surveillance constante des risques en matière de sécurité.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Aucune mesure de sécurité mise en place. Les données sensibles sont vulnérables et exposent l'entreprise à des risques significatifs.	Minimum de mesures de sécurité mis en place mais ne protègent seulement une partie des données. Les protocoles de sécurités sont appliqués de manière incohérente.	Reconnaissance de la sécurité des données SI et mise en place des mesures d'amélioration de la sécurité. Manque de connaissances et de cohérences dans la mise en œuvre des mesures de sécurité. La sensibilisation et la communication sur la sécurité demeurent limitées.	Mises en place des bonnes pratiques. Les données sensibles sont protégées et des protocoles de sécurités sont mis en place. Planification de la formation et de la sensibilisation auprès des collaborateurs.	Mesures de sécurités avancées mis en place comme la détection d'intrusion, la surveillance continue et les cryptages. Les collaborateurs sont sensibilisés et formés. Surveillance constante des risques potentiels pour la sécurité du SI.
VECTEUR 6 – GESTION DES FOURNISSEURS SI	L'entreprise devrait gérer ses relations avec les fournisseurs en définissant des normes de performances et en diversifiant les sources d'approvisionnement.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
La diversité des fournisseurs est limitée, voire inexistante. Dépendance excessive envers un seul fournisseur unique.	Les relations avec les fournisseurs ne sont pas formalisées. Manque de transparence dans la gestion des fournisseurs SI. Les normes de performances ne sont pas définies de manière explicite.	Reconnaissance de la nécessité d'amélioration de la gestion des fournisseurs SI. Mise en place des normes de performances et de la diversification des fournisseurs.	Relation avec les fournisseurs bien établies et gérées. Les contrats sont formalisés, les normes de performances sont claires. Une gestion de surveillance de la qualité et de la conformité des fournisseurs est établie.	Les relations sont actives, contribuent à la réduction des coûts tout en améliorant la qualité des solutions SI.

VECTEUR 7 – PLANIFICATION ET ARCHITECTURE SI	Création d'une vision à long terme pour évoluer le SI de l'entreprise ainsi que la mise en place des structures et des normes d'architectures pour garantir l'alignement avec la stratégie de l'entreprise.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Aucune planification ni architecture SI. Les décisions sont prises de manière réactive sans une vision à long terme.	Planification minimum mais toujours sans une vision à long terme. Les projets sont basés sur des besoins immédiats.	La planification et l'architecture sont en phase d'amélioration. Une planification à long terme est en cours d'élaboration, mais la cohérence dans la mise en œuvre reste à renforcer.	L'entreprise a établi une planification à long terme pour les systèmes d'information, accompagnée d'une architecture bien définie. Les projets SI sont alignés sur la vision stratégique et les normes d'architectures sont respectées.	Une approche stratégique est adoptée pour la planification SI. L'architecture est conçue de manière évolutive afin s'adapter aux besoins changeants de l'entreprise.
VECTEUR 8 – GESTION DE PROJETS SI	L'entreprise devrait planifier, organiser et gérer les projets SI afin d'atteindre leurs objectifs dans les limites de temps et de budget. Pour cela, il est essentiel de former les collaborateurs à la méthodologie agile choisie, de déployer des outils de gestion de projets et d'établir des processus clairement définis.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Absences de processus de gestion de projet. Les projets sont gérés de manière ad hoc, sans méthodologie ni structure définie.	La gestion de projets SI est sporadique et de nombreux de projets échouent en raison de l'absence de processus structurés. Problèmes de budget, d'organisation et de qualité.	Les processus de gestion de projet sont en cours d'amélioration mais des lacunes subsistent dans la formation et la mise en œuvre. Méthodologie agile appliquée mais manque de maîtrise.	Mise en place des processus de gestion de projets efficaces. La gestion est proactive avec des plans de continuité d'activité pour faire face aux événements imprévus.	La gestion de projets est solide avec une amélioration continue des processus. Une méthodologie agile est appliquée avec des rôles bien définis, une priorisation des tâches et le respect des délais. Le budget est planifié et s'aligne avec la stratégie de l'entreprise.
VECTEUR 9 – CONFORMITÉ REGLEMENTAIRE SI	L'entreprise devrait garantir que son SI sont conforment aux lois, règlementations et normes en vigueur dans le domaine de l'informatique et de la protection des données. Une solide conformité réglementaire solide aide à réduire les risques juridiques, à renforcer la réputation de l'entreprise et à protéger les droits des parties prenantes.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
L'entreprise ne respectent pas les réglementations en vigueur, ce qui l'expose à des risques légaux significatifs.	Conformité minimale mais insuffisante. L'entreprise n'est pas pleinement consciente des exigences réglementaires SI.	Reconnaissance de la nécessité d'amélioration de la conformité réglementaire SI. Les exigences sont identifiées mais des lacunes subsistent.	Mise en place des processus pour surveiller et assurer la conformité.	Mise en place des processus proactifs visant à anticiper les évolutions réglementaires et à assurer une conformité rapide. Formation des collaborateurs en matière de conformité.
VECTEUR 10 – GESTION DES INCIDENTS SI	Pour atteindre le plus haut niveau de maturité, il est essentiel que l'entreprise établisse des processus permettant l'identification, la gestion et la résolution efficace des incidents, en plus de former le personnel à ces procédures. La surveillance continue des performances est essentielle pour l'amélioration constante des processus.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Aucun processus de gestion des incidents mis en place. Les incidents sont gérés de manière réactive sans coordination.	La gestion des incidents est sporadique et les procédures ne sont pas bien définies.	Reconnaissance de la nécessité d'améliorer la gestion des incidents. Les processus sont en cours d'améliorations mais des lacunes persistent dans la coordination et la documentation.	Les processus de la gestion des incidents sont opérationnels, avec plusieurs plans de réponse pour divers types d'incident. Coordination efficace.	Les processus sont matures. Les réponses aux incidents sont rapides. L'amélioration continue est intégrée. Les collaborateurs sont formés aux processus.
VECTEUR 11 – GESTION DES RESSOURCES HUMAINES SI	Pour atteindre le plus haut niveau de maturité, l'entreprise devrait recruter, former, motiver et retenir les professionnels en charge des systèmes d'information. Il est essentiel de mettre en place de processus pour recruter des talents qualifiés, de fournir une formation continue, de reconnaître les performances et de favoriser la rétention du personnel SI.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
L'entreprise néglige la gestion des ressources humaines SI. Les collaborateurs SI ne sont pas formés. Un énorme manque de compétence et de motivation.	Un minimum de pratique de gestion des ressources humaines SI mais très peu structurée. Les collaborateurs ont une formation minimum mais insuffisante. Manque de compétence et de motivation.	Reconnaissance de la nécessité d'améliorer la gestion des ressources humaines SI. Les processus sont en phase de développement pour recruter, former et motiver les collaborateurs mais des lacunes subsistent. Planification des formations continues.	Les processus de la gestion des ressources humaines sont efficaces. Les collaborateurs sont bien formés, motivés et aligné sur les objectifs de l'entreprise. Échangent des expériences entre les collaborateurs.	Processus de retour des expériences mis en place pour l'amélioration continue. L'entreprise encourage l'innovation.
VECTEUR 12 – MESURE ET AMÉLIORATION DE LA PERFORMANCE SI	Pour atteindre le plus haut niveau de maturité, l'entreprise devrait mettre en place des mesures, des suivis, des évaluations afin d'améliorer la performance de ses SI. Cela est atteint en définissant des métriques de performances claires, de mettre en place des processus de collecte de données et d'analyser des résultats.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Aucune mesure de performance définie.	Mesure de performances limitées et manque d'une vision holistique de la performance SI. Les mesures sont ad hoc et ne tiennent pas en compte de l'ensemble des processus et des domaines SI.	Reconnaissance de l'importance de mesurer la performance SI. Début d'élaboration des métriques de performance mais des lacunes persistent dans la collecte des données et dans l'analyse.	Les mesures de performance SI établies sont claires et capable d'identifier les domaines qui nécessitent des améliorations.	Les mesures sont avancées et complètes couvrant tous les aspects essentiels de l'environnement SI. Les processus de collecte et d'analyse sont mis en place pour surveiller et mesurer la performance SI en temps réel. Utilisation des outils avancés pour collecter, stocker, et analyser des données de manières efficace. Utilisation de l'analyse prédictive. Les résultats de la mesure sont communiqués à tous les niveaux de l'organisation.

4. Analyse par vecteur

4.1 Stratégie SI

Au sein de l'entreprise VIRTUIX, il existe un manque d'alignement stratégique avec les objectifs globaux de l'entreprise, ce qui entraîne divers défis qui ont un impact sur la gestion des systèmes d'information de l'entreprise. Tout d'abord, elle se concentre sur le développement de scénarii du SimulIT, son produit principal axé sur la cybersécurité. Cela implique l'amélioration de la qualité, de la vitesse de rafraîchissement de l'écran, de la vitesse du contrôle du personnage et des équipements, de la latence, de la réponse du jeu aux actions du personnage ainsi que l'intégration de nouvelles fonctionnalités dans les scénarii, entre autres.

Cependant, malgré cet objectif défini, il existe un écart ou une lacune dans la manière dont cette stratégie contribue aux objectifs globaux de l'entreprise. Par exemple, la société accorde une certaine priorité à l'ajout des nouvelles fonctionnalités à certains scénarii en réaction aux retours des utilisateurs ou en réponse à des erreurs ou des bugs dans le jeu, sans évaluer comment cette décision peut influencer la stratégie de l'entreprise. En d'autres termes, bien que l'entreprise ait une idée précise de ce qu'elle veut accomplir, elle n'a pas encore établi de lien clair entre ces objectifs de développement de scénarios et les objectifs plus larges de l'entreprise, tels que la réalisation de bénéfices, l'expansion sur le marché ou la satisfaction des clients. Cette absence de lien peut entraver la croissance et le succès à long terme de l'entreprise.

De plus, il existe un manque de coordination entre les projets SI et les priorités de l'entreprise. Les ingénieurs systèmes de l'entreprise se focalisent principalement sur la gestion du réseau informatique et le support technique, sans une perspective globale de la manière dont la sécurité de l'information contribue à la réussite de VIRTUIX. Cette absence de coordination peut entraîner des gaspillages de ressources et des investissements inutiles, car les projets SI ne sont pas toujours alignés sur les priorités commerciales.

Bien que la stratégie SI est établie, l'alignement stratégique avec la stratégie d'entreprise est insuffisant. VIRTUIX se trouve actuellement au niveau 2 :

VECTEUR 1 – STRATEGIE SI	La stratégie SI devrait s'aligner sur les objectifs stratégiques de l'entreprise en élaborant une planification et une feuille de route. De plus, une gestion de portefeuille permet de prioriser la création de valeur et garantir l'allocation adéquate de ressources. La stratégie SI est communiquée efficacement à l'ensemble de l'organisation.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Aucune stratégie SI. L'entreprise ne perçoit pas l'importance de l'aligner les SI sur les objectifs de l'entreprise. Les décisions sont prises de façon réactive ou au cas par cas et sans vision stratégique pour les SI.	Bien qu'une stratégie SI existe, elle n'est pas alignée sur la stratégie de l'entreprise. Les décisions sont prises en se basant sur les besoins immédiats sans prise en compte d'une vision à long terme. Manque de coordination entre les projets SI et les priorités de l'entreprise.	Une stratégie SI établie mais partiellement alignée sur les objectifs de l'entreprise. L'entreprise reconnaît l'importance de l'alignement des SI mais des lacunes persistent en matière de l'alignement stratégique.	La stratégie SI est clairement définie et alignée sur la stratégie de l'entreprise. Les décisions sont prises de manière réfléchie en prenant compte à la fois les besoins à court et à long terme.	La stratégie SI est entièrement alignée sur la stratégie de l'entreprise. Il existe des plans à long terme pour le développement des SI accompagnés d'une vision claire. Les SI sont perçus comme un atout stratégique pour l'entreprise.

4.2 Politique et procédure SI

Au sein de l'entreprise, certains politiques et procédures SI sont mis en place, quelques exemples :

- Politique de gestion des mots de passes : les utilisateurs sont tenus de créer des mots de passes forts comprenant au minimum 8 caractères, au moins un caractère spécial, un chiffre, une lettre en majuscule.
- Procédure d'utilisation de VPN : cette procédure guide les utilisateurs sur la manière d'utiliser le VPN en dehors du lieu de travail, en mettant en avant de bonnes pratiques d'utilisation.
- Procédure d'utilisation MFA : cette procédure guide les utilisateurs pour l'installation et l'utilisation d'une application MFA.
- Procédure des accès (physique et virtuel) : elle informe les utilisateurs sur l'utilisation des badges pour accéder au bâtiment, ainsi que l'utilisation d'ordinateurs professionnels, de téléphones professionnels et d'autres appareils tels que les imprimantes ou affranchisseuse.
- Politique de sauvegarde et de récupération des données : cette politique établie les exigences concernant la sauvegarde des données, les délais de rétention des sauvegardes et un plan de récupération en cas de sinistre ou perte de données.

Il n'existe aucune base de données centralisée accessibles aux utilisateurs finaux, ce qui conduit souvent à une méconnaissance de l'existence de certains documents. Bien que certaines procédures soient élaborées, leur communication en interne est soit inexistante, soit limitée à collaborateurs spécifiques. Les employés en prennent généralement connaissance lorsque la nécessité se présente, les obligeant à solliciter le support technique pour obtenir des instructions ou localiser le document requis. De plus, certaines documentations présentent une complexité qui peut être problématique, en particulier pour les lecteurs ayant des connaissances techniques limitées. Cela se traduit souvent par un recours au support technique pour obtenir de l'aide.

Après la création des documentations des politiques et procédures SI, il est constaté qu'elles ne sont ni suivies ni mises à jour. De plus, il n'y a pas de processus de gestion des changements ou d'évolution de ces documents ce qui signifie que les directives et procédures restent statiques, même lorsque des changements sont nécessaires en raison de l'évolution des technologies ou des besoins de l'entreprise. Ce manque de mise à jour peut entraîner des pratiques obsolètes ou inadaptées qui ne répondent pas aux exigences actuelles.

Bien que certaines politiques et procédures soient en place, elles ne sont pas systématiquement communiquées à l'ensemble des collaborateurs et s'avère parfois difficile à suivre. VIRTUIX se trouve actuellement au niveau 3 :

VECTEUR 2 – POLITIQUE ET PROCEDURES SI	Les politiques et les procédures SI favorisent la conformité réglementaire, la sécurité des données et une gestion efficace des systèmes d'information au sein de l'entreprise. Il est important de formaliser ces directives, de les communiquer à l'ensemble des collaborateurs et de mettre en place un suivi pour s'assurer de leur application.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Absence de politiques et procédures en matière de SI. Manque de directives pour la gestion, la sécurité et la conformité SI. Les actions sont prises de manière réactive sans structure ni planification.	Des politiques et procédures existent mais ne sont pas officiellement documentés. Les décisions sont prises de manière ad hoc.	Documentation de certains politiques et procédures mais leur application est incohérente. Les collaborateurs ne sont pas au courant de ces documents ou ne peuvent pas les suivre de manière cohérente. Pas de suivi, ni de révision des documents.	Les politiques et procédures sont documentées et communiqués aux collaborateurs. Il existe une culture de conformité et de respect des directives établies.	Les politiques et les procédures sont régulièrement révisées et améliorées en réponse aux évolutions technologiques et aux besoins de l'entreprise. La conformité, la sécurité et l'efficacité des SI sont constamment renforcées.

4.3 Gestion des ressources SI

VIRTUIX a attiré de nombreux clients suisses avec SimulIT, mais les ressources informatiques de l'entreprise sont surchargées. Le département informatique est composé principalement deux ingénieurs systèmes, dirigés par un Responsable IT. Ces ingénieurs portent plusieurs casquettes, car non seulement ils gèrent le système informatique de l'entreprise, mais ils sont également responsables du support technique. Cela signifie qu'à chaque fois qu'un client ou un employé de VIRTUIX rencontre un problème, il doit contacter directement l'équipe d'ingénieurs, qui réagissent en conséquence. Les interventions téléphoniques varient en durée en fonction de la complexité des problèmes, ce qui signifie que le travail sur les projets planifiés est souvent interrompu.

À court terme, l'entreprise se concentre principalement sur les tâches réactives. Les ingénieurs systèmes sont constamment sollicités pour résoudre des problèmes immédiats, que ce soit pour des clients ayant des besoins de support technique ou pour des incidents de sécurité. Les tâches sont effectuées en réponse à ces demandes, ce qui signifie que les projets planifiés sont souvent négligés ou reportés. Les ingénieurs passent la majeure partie de leur temps à éteindre des incendies plutôt qu'à se concentrer sur des tâches stratégiques.

En ce qui concerne la planification à long terme, il n'y a pratiquement aucune. Il n'existe pas de vision claire pour l'avenir de l'infrastructure informatique de l'entreprise ni de stratégie à long terme pour son développement. Les ingénieurs systèmes réagissent aux problèmes à court terme, mais ils n'ont pas de plan global pour évoluer et s'adapter aux besoins de l'entreprise à mesure qu'elle se développe.

Cette absence de planification à long terme crée un manque de direction et d'alignement entre les ressources informatiques de l'entreprise et ses objectifs commerciaux. La croissance rapide de l'entreprise commence à révéler des fissures dans cette approche, car les problèmes de sécurité et les retards dans la livraison de services deviennent de plus en plus préoccupants. C'est dans ce contexte que le Directeur Général commence à prendre conscience de l'urgence de la situation et de la nécessité de mettre en place une planification stratégique cohérente pour l'entreprise. La croissance rapide de l'entreprise ne peut plus être gérée de manière chaotique. Il commence à comprendre que pour continuer à évoluer, l'entreprise doit investir dans la gestion des ressources informatiques, la cybersécurité et la gouvernance.

VIRTUIX se trouve actuellement au niveau 3 :

VECTEUR 3 – GESTION DE RESSOURCES SI	La gestion des ressources assure une allocation efficace des ressources humaines, financières et technologique, alignées sur les objectifs de l'entreprise. Il est important de mettre en place des processus de gestion des ressources SI, de planifier à court et à long terme et de veiller à l'alignement sur les objectifs de l'entreprise. Une gestion efficiente permet d'optimiser les investissements, de maximiser la productivité et de contribuer de manière significative aux objectifs de l'entreprise.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Les ressources disponibles sont sous-utilisées ou mal gérées. Manque de coordination et planification des ressources.	Gestion de ressources insuffisante ou désorganisée. Les ressources sont utilisées de manière réactive, sans planification à long terme ni l'alignement sur les objectifs de l'entreprise.	Reconnaissance de la nécessité d'amélioration de la gestion des ressources SI mais manque de coordination et de cohérence.	Les ressources sont correctement allouées et gérées selon les besoins grâce à la mise en place des processus de la gestion des ressources SI. Une planification à court et à long terme favorisant l'efficacité et l'alignement stratégique.	Les ressources sont optimisées pour atteindre les objectifs stratégiques tout en minimisant les coûts inutiles. La gestion des ressources SI fait partie de la culture de l'entreprise.

4.4 Gestion des risques

En tant qu'entreprise spécialisée des jeux de simulation liées à la cybersécurité, la gestion des risques est une composante essentielle de la société. Tous les collaborateurs, quel que soit leur niveau dans l'entreprise, sont formés et sensibilisés quant à l'importance de la gestion des risques. Les processus de gestion des risques sont totalement intégrés dans l'ensemble du cycle de vie des projets, de la conception initiale jusqu'à leur mise en œuvre et leur maintenance continue.

Le processus actuel comprend 6 étapes :

1. Identification des risques - Cette phase est dédiée à l'identification des risques potentiels associés au SI et au développement de l'application SimulIT.
2. Évaluation des risques - L'objectif est d'évaluer la probabilité et l'impact de chaque risque, permettant ainsi de classer les risques critiques en fonction de leur importance.
3. Planification de la gestion des risques - Il s'agit de définir le plan d'action pour atténuer, mitiger ou accepter les risques.
4. Mise en œuvre de la gestion des risques - Il s'agit d'intégrer activement la gestion des risques dans le cycle de développement des projets ainsi que l'évolution du SI, tout en surveillant et en adaptant les mesures au fur et à mesure que les circonstances évoluent.
5. Communication et documentation - Toutes les parties prenantes sont tenues informées de l'état des risques et des mesures prises. Une documentation complète est maintenue couvrant l'ensemble du processus de gestion des risques, les évaluations, la stratégie de gestion, les mesures définies ou prises et les rapports de suivi.
6. Revue et rétrospection - Les risques sont régulièrement révisés lors des réunions mensuelles. Les feedbacks jouent un rôle essentiel dans le succès de ce processus de gestion des risques.

En cas d'attaques ou de perturbations majeures touchant VIRTUIX, l'entreprise a élaboré un plan de continuité d'activité[2] (PCA) et un plan de reprise des activités[3] (PRA) détaillés pour faire face à tout incident significatif susceptible d'affecter ses opérations, qu'il s'agisse d'attaques de sécurité, de catastrophes naturelles, ou d'autres situation de crises. Ces plans garantissent que l'entreprise peut maintenir ses activités essentielles et rétablir un fonctionnement normal dans les délais les plus courts possibles.

Le processus du PCA comprend les étapes suivantes :

1. Identification des activités critiques - L'entreprise a identifié les activités essentielles qui doivent être maintenue en cas de perturbation, notamment le support client, la gestion des ventes, la sécurité des produits et la surveillance des systèmes.

[2] *Mettre en place le minimum pour recommencer à travailler.*
[3] *Tout ce qu'il faut faire pour revenir à l'activité normale.*

2. Mise en place de procédures de sauvegarde - Des procédures de sauvegarde ont été mises en place pour garantir la disponibilité des données essentielles. Des sauvegardes régulières sont effectuées pour prévenir toute perte de données.
3. Infrastructure de secours - L'entreprise dispose d'une infrastructure de secours comprenant des centres de données redondants, des liaisons Internet de secours et des systèmes de secours afin de maintenir les opérations en cas de défaillance majeure.
4. Plan de communication d'urgence - Un plan de communication d'urgence a été élaboré pour informer efficacement les employés, les clients et les partenaires en cas de perturbation majeure, assurant ainsi une gestion proactive des situations d'urgence.

Le processus du PRA comprend les étapes suivantes :

1. Évaluation des dégâts et des pertes - L'entreprise évalue les pertes de données, les perturbations opérationnelles, les dégâts et les dommages matériels causés par la perturbation, afin d'obtenir une vision claire de l'impact.
2. Séquence de reprise - Identification des activités critiques qui doivent être rétablies en premier, en fonction de leur importance pour l'entreprise, pour garantir un rétablissement efficace.
3. Restauration de l'infrastructure - Des procédures pour restaurer les systèmes informatiques, les réseaux, l'équipement, et les installations endommagés.
4. Tests et exercices réguliers - Réalisation de test et mise à jour pour s'assurer leur efficacité en cas de perturbation. Ces tests permettent de mettre à jour le plan et de garantir qu'il reste opérationnel en toutes circonstances.

VIRTUIX est une entreprise qui a atteint un niveau de maturité de gestion des risques de niveau 5 :

VECTEUR 4 – GESTION DES RISQUES SI	La gestion des risques consiste à identifier, évaluer et gérer les menaces potentielles aux SI de l'entreprise.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Les risques ne sont pas identifiés ou mal gérés. Peu ou pas de processus mis en place.	Reconnaissance de l'importance de la gestion des risques liés aux SI mais les initiatives sont irrégulières et basées sur des réponses réactives. Les risques ne sont pas évalués et les actions correctives sont prises au cas par cas.	Des processus de gestion des risques sont établis mais pas encore systématisés. La gestion des risques est concentrée seulement sur certains domaines. Manque de communication des risques au sein de l'entreprise.	La gestion des risques est bien établie grâce au processus. Les risques sont évalués de manière systématique et une communication adéquate au sein de l'entreprise existe.	La gestion des risques est intégrée dans toutes les décisions et activités liées aux SI. Les mesures préventives, correctives et mitigation sont mises en place. Des plans de continuité d'activité et de reprise des activités sont établis.

4.5 Sécurité des données SI

Comme mentionné dans la section précédente, VIRTUIX est une entreprise spécialisée dans les jeux de simulation liés à la cybersécurité, par conséquent, la sécurité des données est un domaine maîtrisé. L'entreprise a mis en place des mesures de sécurité avancées, assure une surveillance permanente des risques liés à la Sécurité SI et s'efforce de sensibiliser et de former ses collaborateurs à ces questions.

Voici les mesures de sécurités mises en place :

- Détection d'intrusion - L'entreprise utilise des systèmes de détection d'intrusion avancés pour surveiller en temps réel les activités suspectes sur son réseau. Ces outils sont capables d'identifier rapidement et de signaler les comportements anormaux.
- Surveillance continue - Les ingénieurs assurent une surveillance constante de l'environnement de sécurité à l'aide d'outils de surveillance automatisée afin de détecter les menaces potentielles.
- Cryptages - Toutes les données sensibles sont cryptées, qu'il s'agisse de données en transit ou au repos. Les protocoles de cryptage sont conformes aux meilleures pratiques de l'industrie.
- Authentification multifactorielle (MFA) - Mise en place de MFA pour tous les accès aux systèmes critiques. Cela garantit une vérification d'identité supplémentaire lors de l'accès aux données sensibles.
- Gestion des accès privilégiés (PAM) - Une solution pour protéger les comptes à privilèges tels que les comptes d'administrateurs système. Cela assure une surveillance stricte de l'utilisation de ces comptes et garantir que seuls les administrateurs ont accès à des privilèges étendus.
- Virtual Private Network (VPN) - Une solution pour sécuriser toutes les communications, en particulier lors de l'accès à distance aux systèmes internes.

La sécurité des données est une priorité absolue au de VIRTUIX. Tous les collaborateurs, indépendamment de leur fonction, suivent régulièrement des formations sur les pratiques de sécurité des données. Ces formations englobent la sensibilisation aux menaces actuelles, les bonnes pratiques en matière de mots de passe, à la gestion des données sensibles, et à la détection des tentatives d'hameçonnage.

VIRTUIX a atteint un niveau de maturité de sécurité des données SI de niveau 5 :

VECTEUR 5 – SECURITÉ DES DONNÉES SI	La sécurité des données SI se concentre à la protection des informations sensibles et critiques de l'entreprise, la sensibilisation des collaborateurs, la veille technologique ainsi que la surveillance constante des risques en matière de sécurité.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Aucune mesure de sécurité mise en place. Les données sensibles sont vulnérables et exposent l'entreprise à des risques significatifs.	Minimum de mesures de sécurité mis en place mais ne protègent seulement une partie des données. Les protocoles de sécurités sont appliqués de manière incohérente.	Reconnaissance de la sécurité des données SI et mise en place des mesures d'amélioration de la sécurité. Manque de connaissances et de cohérences dans la mise en œuvre des mesures de sécurité. La sensibilisation et la communication sur la sécurité demeurent limitées.	Mises en place des bonnes pratiques. Les données sensibles sont protégées et des protocoles de sécurités sont mis en place. Planification de la formation et de la sensibilisation auprès des collaborateurs.	Mesures de sécurités avancées mis en place comme la détection d'intrusion, la surveillance continue et les cryptages. Les collaborateurs sont sensibilisés et formés. Surveillance constante des risques potentiels pour la sécurité du SI.

4.6 Gestion des fournisseurs SI

Actuellement, VIRTUIX repose de manière significative sur un seul fournisseur unique pour répondre à ses besoins en matière de systèmes d'information, ce qui la rend vulnérable aux risques potentiels, tels qu'une réalisation de contrat ou des coûts élevés. Pour atténuer ces risques et augmenter sa flexibilité, l'entreprise a entrepris un processus de diversification de ses fournisseurs SI.

Voici le processus en cours de développement :

1. Évaluation des besoins - Cette étape consiste à identifier les besoins SI et de fournisseurs, en identifiant les services essentiels.
2. Identification de nouveaux fournisseurs - Il s'agit de mener des recherches pour repérer d'autres fournisseurs potentiels susceptibles de répondre à ses besoins en matière de SI. Les fournisseurs potentiels peuvent être des fournisseurs locaux ou internationaux.
3. Appel d'offres - L'entreprise lance un appel d'offres pour solliciter des propositions de la part des fournisseurs potentiels. Cela permet de comparer les coûts, la qualité, les services et la flexibilité.
4. Plan de transition - Un plan d'action pour migrer progressivement vers de nouveaux fournisseurs tout en minimisant les perturbations opérationnelles.
5. Gestion des fournisseurs SI - Mettre en place des processus de gestion de la relation fournisseur SI pour s'assurer qu'ils répondent aux attentes et aux normes de qualité de l'entreprise.

VIRTUIX se trouve actuellement à un niveau de maturité de gestion des fournisseurs SI de niveau 1 :

VECTEUR 6 – GESTION DES FOURNISSEURS SI	L'entreprise devrait gérer ses relations avec les fournisseurs en définissant des normes de performances et en diversifiant les sources d'approvisionnement.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
La diversité des fournisseurs est limitée, voire inexistante. Dépendance excessive envers un seul fournisseur unique.	Les relations avec les fournisseurs ne sont pas formalisées. Manque de transparence dans la gestion des fournisseurs SI. Les normes de performances ne sont pas définies de manière explicite.	Reconnaissance de la nécessité d'amélioration de la gestion des fournisseurs SI. Mise en place des normes de performances et de la diversification des fournisseurs.	Relation avec les fournisseurs bien établies et gérées. Les contrats sont formalisés, les normes de performances sont claires. Une gestion de surveillance de la qualité et de la conformité des fournisseurs est établie.	Les relations sont actives, contribuent à la réduction des coûts tout en améliorant la qualité des solutions SI.

4.7 Planification et architecture SI

Actuellement, VIRTUIX a une planification minimale en ce qui concerne ses systèmes d'information. Les décisions sont réactives, basées sur des besoins immédiats, sans une vision claire à long terme.

Sur le plan technique, l'entreprise se trouve confrontée à plusieurs défis dus à une planification minimale et à l'absence d'une vision à long terme :

- Manque de scalabilité - Les serveurs actuels sont dimensionnés pour répondre aux besoins actuels, mais la croissance rapide des données liées aux simulations de cybersécurité a engendré des goulots d'étranglement. En l'absence de planification à long terme, l'entreprise peine à anticiper et à gérer cette croissance.
- Incompatibilité des systèmes - Les nouvelles fonctionnalités ajoutées au logiciel SimulIT n'ont pas été intégrée de manière cohérente dans l'architecture existante, rendant les systèmes hétérogènes et incompatibles, ce qui entraîne des problèmes de performance et de maintenance.
- Ressources inefficacement allouées - En l'absence d'une planification, les ressources informatiques sont allouées de manière réactive, entraînant par exemple l'achat de serveurs supplémentaires sans tenir compte de la capacité réelle requise. Il y avait une redondance inutile de ressources et cela a entraîné un gaspillage de ressources.
- Réactivité aux demandes des clients - La réactivité a parfois conduit à des développements rapides et non coordonnés, aboutissant à des fonctionnalités qui ne s'intègrent pas bien dans l'ensemble du système.
- Complexité de maintenance - En raison de l'architecture hétérogène et des ajouts ad hoc, la maintenance est devenue complexe, obligeant les ingénieurs à gérer différents systèmes avec des configurations différentes, augmentant ainsi les risques d'erreurs et les temps d'arrêt.

Actuellement, VIRTUIX se trouve à un niveau de maturité de planification et d'architecture SI de niveau 2 :

VECTEUR 7 – PLANIFICATION ET ARCHITECTURE SI	Création d'une vision à long terme pour évoluer le SI de l'entreprise ainsi que la mise en place des structures et des normes d'architectures pour garantir l'alignement avec la stratégie de l'entreprise.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Aucune planification ni architecture SI. Les décisions sont prises de manière réactive sans une vision à long terme.	Planification minimum mais toujours sans une vision à long terme. Les projets sont basés sur des besoins immédiats.	La planification et l'architecture sont en phase d'amélioration. Une planification à long terme est en cours d'élaboration, mais la cohérence dans la mise en œuvre reste à renforcer.	L'entreprise a établi une planification à long terme pour les systèmes d'information, accompagnée d'une architecture bien définie. Les projets SI sont alignés sur la vision stratégique et les normes d'architectures sont respectées.	Une approche stratégique est adoptée pour la planification SI. L'architecture est conçue de manière évolutive afin s'adapter aux besoins changeants de l'entreprise.

4.8 Gestion de projets SI

La gestion irrégulière des projets SI entraîne des échecs fréquents en raison de l'absence de processus structurés. L'entreprise VIRTUIX semble être consciente des problèmes liés à la gestion des projets SI mais n'a pas encore élaboré des processus de gestion de projet pour les résoudre. La croissance de l'entreprise a besoin une amélioration significative de sa maturité de gestion de projets SI pour mieux gérer les besoins de ses employés et la prestation de services à ses clients. Voici quelques points qui suggèrent un manque de maturité sur ce vecteur :

- Documentation minimale
- Gestion réactive plutôt que proactive
- Manque de clarté dans les rôles et responsabilités
- Croissance non maîtrisée

L'entreprise a décidé de lancer une élaboration des processus de gestions de projets SI. Les étapes qu'ils aimeraient mettre en place sont les suivantes :

1. Analyser les projets passés - Cette étape est un point crucial afin de mettre en évidence les raisons des échecs et les domaines qui nécessitent une amélioration.
2. Évaluation des besoins - Il s'agit d'identifier les besoins de chaque projet ainsi que les ressources, les coûts, les délais et les risques.
3. Recherche sur différente méthodologie agile sur la gestion des projets - Cette phase consiste à se former sur des méthodologies existantes afin de mieux maîtriser le bon fonctionnement d'une gestion de projets.
4. Gestion de la qualité - Il s'agit de mettre en place des processus de contrôle de qualité pour s'assurer que les livrables répondent aux normes.

L'entreprise VIRTUIX se trouve à un niveau de maturité de gestion de projets SI de niveau 2 :

VECTEUR 8 – GESTION DE PROJETS SI	L'entreprise devrait planifier, organiser et gérer les projets SI afin d'atteindre leurs objectifs dans les limites de temps et de budget. Pour cela, il est essentiel de former les collaborateurs à la méthodologie agile choisie, de déployer des outils de gestion de projets et d'établir des processus clairement définis.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Absences de processus de gestion de projet. Les projets sont gérés de manière ad hoc, sans méthodologie ni structure définie.	La gestion de projets SI est sporadique et de nombreux de projets échouent en raison de l'absence de processus structurés. Problèmes de budget, d'organisation et de qualité.	Les processus de gestion de projet sont en cours d'amélioration mais des lacunes subsistent dans la formation et la mise en œuvre. Méthodologie agile appliquée mais manque de maîtrise.	Mise en place des processus de gestion de projets efficaces. La gestion est proactive avec des plans de continuité d'activité pour faire face aux événements imprévus.	La gestion de projets est solide avec une amélioration continue des processus. Une méthodologie agile est appliquée avec des rôles bien définis, une priorisation des tâches et le respect des délais. Le budget est planifié et s'aligne avec la stratégie de l'entreprise.

4.9 Conformité règlementaire SI

L'entreprise reconnaît l'importance de la conformité aux lois et règlementations liées à l'informatique et à la protection des données. Voici les mesures prises :

- Audit de conformité - L'entreprise collabore avec une société d'audit externe spécialisée en cybersécurité qui a mené un audit complet des systèmes d'information de l'entreprise pour évaluer la conformité aux lois.
- Surveillance active d'évolution des lois - Il s'agit d'une surveillance régulière des diverses sources d'information et un abonnement à des mises à jour automatiques concernant les nouvelles règlementations.
- Formation et sensibilisation - Les collaborateurs reçoivent régulièrement des formations sur la sécurité de l'information. Les sessions comprennent des modules sur la protection des données, la sensibilisation aux menaces, et les bonnes pratiques de sécurité. De plus, les employés sont informés sur la manière de gérer l'information sensibles, d'utiliser des mots de passe forts et de signaler les incidents de sécurité.
- Mise en conformité continue - Il s'agit des processus pour examiner les évolutions légales et la mise en conformité du SI de l'entreprise.

L'entreprise VIRTUIX se trouve actuellement à un niveau de maturité de niveau 4 :

VECTEUR 9 – CONFORMITÉ REGLEMENTAIRE SI		L'entreprise devrait garantir que son SI sont conforment aux lois, règlementations et normes en vigueur dans le domaine de l'informatique et de la protection des données. Une solide conformité réglementaire solide aide à réduire les risques juridiques, à renforcer la réputation de l'entreprise et à protéger les droits des parties prenantes.		
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
L'entreprise ne respectent pas les réglementations en vigueur, ce qui l'expose à des risques légaux significatifs.	Conformité minimale mais insuffisante. L'entreprise n'est pas pleinement consciente des exigences réglementaires SI.	Reconnaissance de la nécessité d'amélioration de la conformité réglementaire SI. Les exigences sont identifiées mais des lacunes subsistent.	Mise en place des processus pour surveiller et assurer la conformité.	Mise en place des processus proactifs visant à anticiper les évolutions réglementaires et à assurer une conformité rapide. Formation des collaborateurs en matière de conformité.

4.10 Gestion des incidents SI

L'entreprise reconnaît la nécessité d'améliorer la gestion des incidents de sécurité de l'information. Ci-dessous figurent les processus de l'entreprise :

- Plans de réponse aux incidents - Ces plans détaillent les étapes à entreprendre en cas d'incident. Ils incluent l'isolement de systèmes compromis, la restauration des données, l'application de correctifs de sécurité, la communication avec les parties prenantes, et la gestion des médias.
- Formation des collaborateurs - Il s'agit de la sensibilisation et de la formation des employés grâce à des scénarios d'incident et des exercices de simulations.
- Gestion des incidents - Ces processus englobent la détection, la notification, l'investigation, la résolution et la communication des incidents.
- Documentation - L'entreprise maintient une documentation de tous les aspects de la gestion des incidents, notamment les mesures prises et les leçons apprises.

Bien que des processus aient été instaurés, l'entreprise éprouve des difficultés à pleinement maîtriser ces processus, car elle peine à passer d'une approche réactive à une approche plus proactive. Par exemple, une tentative d'intrusion ait été détectée dans le réseau de VIRTUIX. Les ingénieurs réagissent immédiatement en isolant le système affecté, et en lançant une enquête préliminaire. Cependant, le processus de notification des parties prenantes, y compris les clients, est encore en cours d'amélioration, ce qui entraîne des défis dans la communication, qui n'est pas aussi fluide qu'elle le devrait.

L'entreprise VIRTUIX se situe à un niveau de maturité de gestion de incidents SI de niveau 3 :

VECTEUR 10 – GESTION DES INCIDENTS SI	Pour atteindre le plus haut niveau de maturité, il est essentiel que l'entreprise établisse des processus permettant l'identification, la gestion et la résolution efficace des incidents, en plus de former le personnel à ces procédures. La surveillance continue des performances est essentielle pour l'amélioration constante des processus.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Aucun processus de gestion des incidents mis en place. Les incidents sont gérés de manière réactive sans coordination.	La gestion des incidents est sporadique et les procédures ne sont pas bien définies.	Reconnaissance de la nécessité d'améliorer la gestion des incidents. Les processus sont en cours d'améliorations mais des lacunes persistent dans la coordination et la documentation.	Les processus de la gestion des incidents sont opérationnels, avec plusieurs plans de réponse pour divers types d'incident. Coordination efficace.	Les processus sont matures. Les réponses aux incidents sont rapides. L'amélioration continue est intégrée. Les collaborateurs sont formés aux processus.

4.11 Gestion des ressources humaines SI

L'entreprise a embauché deux ingénieurs systèmes pour gérer le parc informatique de VIRTUIX. Toutefois, leurs responsabilités ne sont pas clairement définies et il n'existe pas de processus formels pour la gestion des ressources humaines en matière de sécurité de l'information. Ci-dessous figurent les défis que rencontre l'entreprise :

- Formation insuffisante en cybersécurité : Les ingénieurs systèmes ont une formation limitée en cybersécurité et acquièrent des compétences sur le terrain en réagissant aux incidents ou aux perturbations.
- Motivation réduite : En raison de leur charge de travail liée à la gestion total du parc informatique et au support technique, les ingénieurs ont peu de temps de pour se former en cybersécurité, ce qui affecte leur niveau de motivation.
- Responsabilités ambiguës : Les ingénieurs peinent à définir leurs responsabilités car ils doivent jongler entre plusieurs rôles au sein de l'entreprise.
- Manque de personnel : Seulement deux ingénieurs systèmes sont chargés de la gestion complète du parc informatique de l'entreprise.

En outre, les processus de gestion des ressources humaines SI ne sont pas formalisés :

- Processus de Gestion des Responsabilités SI : Un processus qui définit explicitement les rôles et responsabilités en matière de gestion du SI. Toutefois, les ingénieurs systèmes sont souvent contraints d'accomplir des tâches car ils doivent répondre aux incidentes, quelle que soit la charge du travail. De même, au niveau de l'évolution du SI, ils doivent faire face aux exigences afin d'éviter tout dysfonctionnement du réseau ou d'autres problèmes.
- Processus de motivation et d'incitation - Un processus pour motiver, reconnaître et récompenser les employés. Toutefois, les ingénieurs ne reçoivent pas de reconnaissance en raison de la charge de travail écrasante de l'entreprise, qui ne laisse que peu de temps pour la reconnaissance.
- Processus de suivi de la formation : Un processus permettant d'évaluer l'efficacité des programmes de formations et de garantir que le personnel acquiert les compétences nécessaires. Cependant, les ingénieurs n'ont pas le temps de suivre ces formations, ce qui rend difficile l'évaluation de leur efficacité.

L'entreprise VIRTUIX se trouve à un niveau de maturité de gestion de ressources humaines SI de niveau 2 :

VECTEUR 11 – GESTION DES RESSOURCES HUMAINES SI		Pour atteindre le plus haut niveau de maturité, l'entreprise devrait recruter, former, motiver et retenir les professionnels en charge des systèmes d'information. Il est essentiel de mettre en place de processus pour recruter des talents qualifiés, de fournir une formation continue, de reconnaître les performances et de favoriser la rétention du personnel SI.		
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
L'entreprise néglige la gestion des ressources humaines SI. Les collaborateurs SI ne sont pas formés. Un énorme manque de compétence et de motivation.	Un minimum de pratique de gestion des ressources humaines SI mais très peu structurée. Les collaborateurs ont une formation minimum mais insuffisante. Manque de compétence et de motivation.	Reconnaissance de la nécessité d'améliorer la gestion des ressources humaines SI. Les processus sont en phase de développement pour recruter, former et motiver les collaborateurs mais des lacunes subsistent. Planification des formations continues.	Les processus de la gestion des ressources humaines sont efficaces. Les collaborateurs sont bien formés, motivés et aligné sur les objectifs de l'entreprise. Échangent des expériences entre les collaborateurs.	Processus de retour des expériences mis en place pour l'amélioration continue. L'entreprise encourage l'innovation.

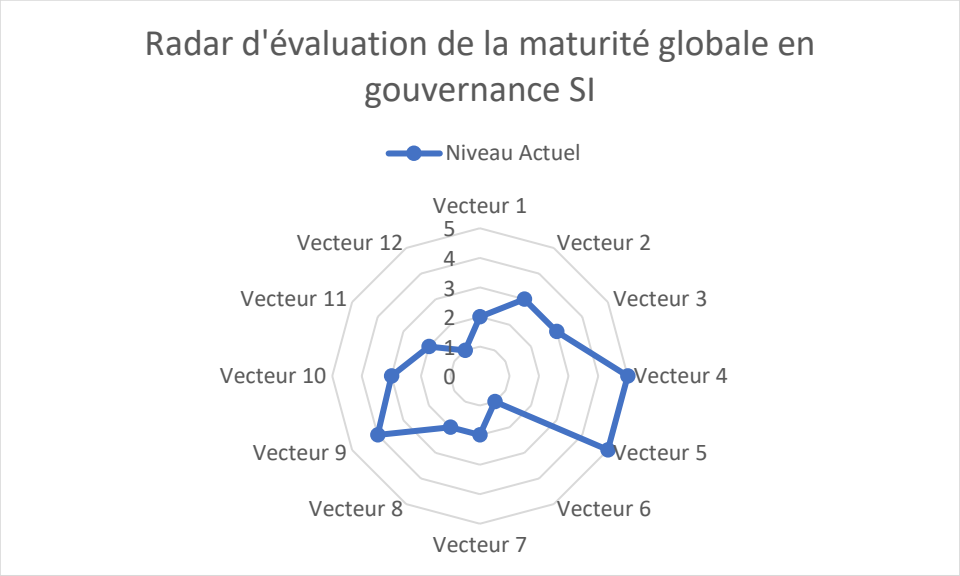
4.12 Mesure et amélioration de la performance SI

L’entreprise n’a pas mis en place de mesures de performance pour évaluer l’efficacité de son SI. Les opérations liées au SI sont principalement gérées de manière réactive, sans l’utilisation de données quantitatives pour évaluer la performance telles que la disponibilité des systèmes, la qualité des services informatiques, les coûts liés à la technologie de l'information, ou la satisfaction des utilisateurs. En conséquence, l'entreprise opère dans l'obscurité en ce qui concerne la performance de son SI.

L’entreprise VIRTUIX se situe actuellement à un niveau de maturité de niveau 1 :

VECTEUR 12 – MESURE ET AMÉLIORATION DE LA PERFORMANCE SI	Pour atteindre le plus haut niveau de maturité, l’entreprise devrait mettre en place des mesures, des suivis, des évaluations afin d’améliorer la performance de ses SI. Cela est atteint en définissant des métriques de performances claires, de mettre en place des processus de collecte de données et d’analyser des résultats.			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Aucune mesure de performance définie.	Mesure de performances limitées et manque d’une vision holistique de la performance SI. Les mesures sont ad hoc et ne tiennent pas en compte de l’ensemble des processus et des domaines SI.	Reconnaissance de l’importance de mesurer la performance SI. Début d’élaboration des métriques de performance mais des lacunes persistent dans la collecte des données et dans l’analyse.	Les mesures de performance SI établies sont claires et capable d’identifier les domaines qui nécessitent des améliorations.	Les mesures sont avancées et complètes couvrant tous les aspects essentiels de l’environnement SI. Les processus de collecte et d’analyse sont mis en place pour surveiller et mesurer la performance SI en temps réel. Utilisation des outils avancés pour collecter, stocker, et analyser des données de manières efficace. Utilisation de l’analyse prédictive. Les résultats de la mesure sont communiqués à tous les niveaux de l’organisation.

5. Conclusion



VIRTUIX fait face à plusieurs défis majeurs dans sa gestion des systèmes d'information (SI) et de cybersécurité. Au niveau de la stratégie SI, il y a un manque d'alignement avec les objectifs de l'entreprise, une coordination insuffisante entre les projets SI et un manque de planification à long terme.

En ce qui concerne la sécurité des données SI, l'entreprise a mis en place des mesures avancées, mais des lacunes subsistent dans la gestion des incidents. La gestion des fournisseurs SI est en cours de diversification pour réduire les risques, mais est encore à un stade préliminaire.

La gestion des projets SI est actuellement réactive, entraînant des échecs fréquents. VIRTUIX travaille sur l'amélioration de ses processus de gestion de projet. En matière de conformité règlementaire SI, l'entreprise collabore avec des sociétés d'audit externes et forme régulièrement ses employés en sécurité de l'information.

Enfin, la gestion des ressources humaines SI est confrontée à des défis tels que des formations insuffisantes, des responsabilités ambiguës et un manque de personnel. Les processus de gestion des ressources humaines SI ne sont pas formalisés, entraînant des problèmes de compétence et de motivation.

Afin de remédier à ces difficultés, VIRTUIX doit prendre des mesures significatives pour résoudre ces problèmes et garantir sa croissance à long terme tout en maintenant la sécurité de ses systèmes d'information. Voici les vecteurs clés à améliorer :

1. **Stratégie SI** - Aligner la stratégie SI avec les objectifs commerciaux pour une croissance durable. Pour ce faire, VIRTUIX devrait établir un lien clair entre l'évolution du SI, les objectifs de développement de scénarios et les objectifs commerciaux. Cela peut être accompli en évaluant systématiquement comment chaque décision relative au développement de scénarios contribue à la réalisation des bénéfices, à l'expansion du marché et à la satisfaction des clients. De plus, une meilleure coordination entre les projets SI et les priorités de l'entreprise est nécessaire pour éviter les gaspillages de ressources.

2. **Politique et procédure SI** - VIRTUIX devrait mettre en place une base de données centralisée pour rendre les politiques et procédures SI facilement accessibles à tous les collaborateurs. De plus, la communication interne des politiques et procédures doit être renforcée pour garantir que tous les employés en sont informés. Il est également important d'établir un processus de gestion des changements et de révision des documents pour maintenir les politiques et procédures à jour.
3. **Gestion des Ressources Humaines SI** - : L'entreprise doit investir dans la formation en cybersécurité de ses ingénieurs systèmes et clarifier leurs rôles et responsabilités. Des incitations à la formation et à la certification en cybersécurité peuvent motiver les employés à développer leurs compétences. De plus, la création de processus de gestion des ressources humaines SI structurés peut aider à définir les responsabilités et à garantir que les employés disposent du temps nécessaire pour se former.
4. **Gestion des Projets SI** - VIRTUIX doit mettre en place des processus de gestion de projet formels pour planifier, exécuter et surveiller les projets SI. Cela inclut la documentation complète des projets, la définition claire des rôles et responsabilités, et la priorisation des projets en fonction de leur importance stratégique. En outre, des méthodologies de gestion de projet, telles que les approches agiles, peuvent être mises en œuvre pour améliorer la gestion des projets.
5. **Planification et Architecture SI** - L'entreprise doit élaborer une stratégie SI à long terme pour mieux gérer la croissance et garantir la scalabilité. L'harmonisation des systèmes existants et des nouvelles fonctionnalités est cruciale pour éviter les problèmes de performance et de maintenance. Une allocation de ressources plus efficace basée sur la planification est nécessaire pour éviter le gaspillage.
6. **Gestion des Incidents SI** - Améliorer la gestion des incidents et la communication avec les parties prenantes.
7. **Gestion des Fournisseurs SI** - VIRTUIX devrait diversifier ses fournisseurs SI pour réduire sa dépendance à un seul fournisseur. Cela nécessite une évaluation des besoins, la recherche de nouveaux fournisseurs, la comparaison des coûts et la mise en place de plans de transition pour minimiser les perturbations opérationnelles. La gestion continue de la relation fournisseur SI est essentielle pour garantir qu'ils répondent aux normes de qualité de l'entreprise.
8. **Conformité Règlementaire SI** - L'entreprise doit continuer à surveiller les évolutions légales et à se conformer aux lois et réglementations liées à la sécurité de l'information. Cela inclut la mise en place de processus de gestion de la conformité, l'audit régulier et la formation continue des employés.
9. **Sécurité des Données SI** - Maintenir des mesures de sécurité avancées et sensibiliser les employés.
10. **Gestion des Risques SI** - Intégrer la gestion des risques dans toutes les activités liées aux SI.

En se concentrant sur ces domaines, VIRTUIX améliorera sa gestion des SI, renforcera sa compétitivité et minimisera les risques.