**Partie 1 :** Résumé exécutif (2 pts) Dans cette partie vous devez produire un résumé managérial des risques identifiés suite à votre étude.

Voici un résumé des risques identifiés suite à l'étude de la sécurité de l'imprimante Imprim20000 :

* Risque de piratage : l'imprimante étant connectée à Internet, elle peut être la cible de tentatives de piratage visant à accéder aux données qu'elle traite ou à la contrôler à distance.
* Risque de fuite de données : si les données traitées par l'imprimante ne sont pas correctement protégées, il y a un risque qu'elles soient divulguées à des tiers non autorisés.
* Risque de perte de données : il y a un risque que les données stockées sur l'imprimante soient perdues en cas de défaillance du matériel ou de problème de logiciel.
* Risque de non-conformité réglementaire : si les règles de sécurité en vigueur ne sont pas respectées, il y a un risque de non-conformité à la réglementation en vigueur, ce qui peut entraîner des sanctions et des pénalités pour T-Acourt.

Pour gérer ces risques, il est recommandé de mettre en place des mesures de sécurité adéquates, telles que la mise en place d'un système de gestion des identités et des accès, l'application de mises à jour de sécurité régulières, l'encryptage des communications et la mise en place d'un système de journalisation et de surveillance. Il est également important de former les utilisateurs aux bonnes pratiques de sécurité et de mettre en place des politiques et des procédures de sécurité claires et communiquées à tous les employés de T-Acourt.

Voici d'autres risques qui pourraient être pris en compte dans l'étude de la sécurité de l'imprimante Imprim20000 :

* Risque de défaillance matérielle : il y a un risque que le matériel de l'imprimante tombe en panne, ce qui pourrait entraîner une perte de données ou une interruption de l'activité.
* Risque de non-conformité aux normes de qualité : si les imprimantes ne sont pas fabriquées ou entretenues selon les normes de qualité en vigueur, il y a un risque que leur performance ou leur durée de vie soient affectées.
* Risque de non-respect de la réglementation environnementale : si l'imprimante ne respecte pas les réglementations environnementales en vigueur, T-Acourt pourrait être sanctionné et perdre en crédibilité auprès de sa clientèle.
* Risque de concurrence déloyale : si des concurrents de T-Acourt proposent des produits similaires à des prix inférieurs, il y a un risque de perte de parts de marché pour T-Acourt.
* Risque de changement de la demande du marché : il y a un risque que la demande pour les imprimantes de T-Acourt fluctue en fonction de facteurs externes, tels que l'évolution de la technologie ou les changements de mode de consommation.

Il est important de prendre en compte tous ces risques dans l'étude de la sécurité de l'imprimante Imprim20000 et de mettre en place des mesures adéquates pour les gérer.

1. Risques financiers : Il y a un risque que les données financières de l'entreprise soient volées ou utilisées de manière non autorisée, ce qui pourrait entraîner une perte financière importante pour l'entreprise.
2. Risques de sécurité informatique : L'entreprise est exposée à des risques de sécurité informatique tels que les attaques informatiques ciblées et les vols de données. Ces risques peuvent entraîner des pertes financières importantes et endommager la réputation de l'entreprise.
3. Risques liés aux actifs humains : L'entreprise est exposée au risque de perte de ses employés clés en raison de départs ou de décès. Cela pourrait affecter négativement la performance de l'entreprise.
4. Risques liés aux actifs clients : L'entreprise est exposée au risque de perte de clients en raison de la concurrence ou de changements dans les besoins des clients. Cela pourrait affecter négativement les revenus de l'entreprise.

**Partie 2** : Une synthèse de vos recommandations au management afin que ces risques soient traités à un niveau acceptable. (2 pts)

Il est important de mettre en place des mesures de sécurité pour protéger l'imprimante Imprim20000 et les données qui y sont traitées. Voici quelques recommandations qui pourraient être mises en place :

* Mettre en place un système de gestion des identités et des accès (Identity and Access Management, IAM) pour contrôler qui a accès à l'imprimante et à quelles parties de celle-ci. Cela peut inclure l'utilisation de codes d'accès uniques pour chaque utilisateur et la mise en place de règles d'accès basées sur les rôles de chaque utilisateur.
* Appliquer des mises à jour de sécurité régulières pour corriger les failles de sécurité connues et protéger l'imprimante contre les attaques éventuelles. Cela peut être fait en utilisant le système de mises à jour en direct depuis le cloud de T-Acourt.
* Encrypter les communications entre l'imprimante et les autres appareils qui y sont connectés, afin de protéger les données transmises contre les écoutes non autorisées.
* Mettre en place un système de journalisation et de surveillance pour enregistrer les activités de l'imprimante et permettre une détection précoce des activités suspectes.
* Former les utilisateurs de l'imprimante aux bonnes pratiques de sécurité, afin de les sensibiliser aux risques de piratage et de leur montrer comment protéger leurs données et leur appareil.

Il est également important de mettre en place des politiques et des procédures de sécurité claires et de les communiquer à tous les employés de T-Acourt, afin de s'assurer que tout le monde comprend les mesures de sécurité mises en place et les respecte.

Voici une synthèse des recommandations qui pourraient être faites au management de T-Acourt afin de traiter les risques liés à l'imprimante Imprim20000 à un niveau acceptable :

* Mettre en place un système de gestion des identités et des accès (Identity and Access Management, IAM) pour contrôler qui a accès à l'imprimante et à quelles parties de celle-ci. Cela peut inclure l'utilisation de codes d'accès uniques pour chaque utilisateur et la mise en place de règles d'accès basées sur les rôles de chaque utilisateur.
* Appliquer des mises à jour de sécurité régulières pour corriger les failles de sécurité connues et protéger l'imprimante contre les attaques éventuelles. Cela peut être fait en utilisant le système de mises à jour en direct depuis le cloud de T-Acourt.
* Encrypter les communications entre l'imprimante et les autres appareils qui y sont connectés, afin de protéger les données transmises contre les écoutes non autorisées.
* Mettre en place un système de journalisation et de surveillance pour enregistrer les activités de l'imprimante et permettre une détection précoce des activités suspectes.
* Former les utilisateurs de l'imprimante aux bonnes pratiques de sécurité, afin de les sensibiliser aux risques de piratage et de leur montrer comment protéger leurs données et leur appareil.
* Mettre en place des politiques et des procédures de sécurité claires et les communiquer à tous les employés de T-Acourt, afin de s'assurer que tout le monde comprend les mesures de sécurité mises en place et les respecte.
* Prévoir des budgets suffisants pour l'achat de matériel de qualité et pour la maintenance de l'imprimante, afin de minimiser les risques de défaillance matérielle.
* Veiller à respecter les normes de qualité et les réglementations environnementales en vigueur, afin d'éviter les sanctions et les pertes de crédibilité.
* Surveiller l'environnement concurrentiel et être proactif dans l'adaptation de l'offre de T-Acourt en fonction de l'évolution de la demande du marché.

En mettant en place ces mesures, T-Acourt pourra gérer les risques liés à l'imprimante Imprim20000 à un niveau acceptable et assurer la sécurité de ses données et de ses activités.

**Partie 3** : Analyse de risque (16 pts)

Il semble que vous êtes le Responsable de la Sécurité des Systèmes d'Information (RSSI) de la startup T-Acourt, et que vous êtes sollicité en début de projet pour le développement de leur nouvelle imprimante industrielle automatisée, Imprim20000. Comme il y a de plus en plus de cas de vols d'information et de piratage des objets connectés, vous êtes inquiet pour la sécurité de cette imprimante.

Voici quelques éléments à prendre en compte pour la sécurité de cette imprimante :

* Sécurité physique : il est important de s'assurer que l'accès physique à l'imprimante est contrôlé et sécurisé, par exemple en utilisant des codes d'accès spécifiques pour chaque utilisateur et en protégeant les ports de connexion physique avec des dispositifs de verrouillage.
* Sécurité réseau : il est important de s'assurer que l'imprimante est connectée de manière sécurisée au réseau, par exemple en utilisant des protocoles de sécurité tels que SSL/TLS. Il est également important de mettre en place des mesures de sécurité pour protéger l'imprimante contre les attaques réseau, comme l'utilisation de pare-feu et de logiciels antivirus.
* Mises à jour de sécurité : il est important de mettre régulièrement à jour le système d'exploitation de l'imprimante et de télécharger les patches de sécurité pour corriger les bugs et renforcer la sécurité de l'imprimante.
* Gestion des accès : il est important de mettre en place une stratégie de gestion des accès pour contrôler qui a accès à l'imprimante et à quelles fonctionnalités. Cela peut inclure l'utilisation de rôles et de permissions spécifiques pour chaque utilisateur.
* Sauvegarde des données : il est important de mettre en place des stratégies de sauvegarde des données pour protéger les données de l'imprimante en cas de perte ou de dommages.

En tant que RSSI, vous devriez également être en mesure de sensibiliser le reste de l'équipe à la sécurité des systèmes d'information et de les aider à adopter des pratiques sécurisées au quotidien.

**Étape 1 : Identifier les actifs de l’entreprise.**

Les actifs de l'entreprise T-Acourt peuvent être regroupés en plusieurs catégories:

1. Actifs financiers: il s'agit des ressources financières de l'entreprise, comme les liquidités, les placements, les créances clients, etc.
2. Actifs immatériels: il s'agit des éléments intangibles qui ont une valeur pour l'entreprise, comme les marques, les licences, les brevets, les savoir-faire, etc.
3. Actifs matériels: il s'agit des équipements, des outils et des installations de l'entreprise, comme les ordinateurs, les imprimantes, les locaux, etc.
4. Actifs humains: il s'agit des employés et des dirigeants de l'entreprise, ainsi que de leurs compétences et de leur savoir-faire.
5. Actifs clients: il s'agit des relations et des partenariats que l'entreprise a établis avec ses clients.

En ce qui concerne la startup T-Acourt, les actifs de l'entreprise pourraient inclure l'imprimante industrielle automatisée Imprim20000, les licences et brevets associés à cette imprimante, les employés de l'entreprise, les immeubles et l'équipement utilisés pour le développement et la production de l'imprimante, et toutes les marques et autres actifs intangibles associés à l'entreprise.

**Étape 2 : Identifier la valeur de chaque actif à travers les critères en termes de Disponibilité, Intégrité et Confidentialité. Ces valeurs vont vous permettre ensuite d’établir l’impact sur la société en cas d’exécution d’un scénario à risque.**

* Disponibilité : la disponibilité d'un actif désigne sa capacité à être utilisé de manière efficace et opportune. Par exemple, pour l'imprimante industrielle Imprim20000, la disponibilité serait importante car si l'imprimante est indisponible, cela peut entraîner des retards de production et des pertes financières pour l'entreprise.
* Intégrité : l'intégrité d'un actif désigne sa capacité à être exact et complet. Par exemple, pour l'imprimante Imprim20000, l'intégrité serait importante car si l'imprimante ne produit pas des impressions de qualité, cela peut entraîner des pertes financières pour l'entreprise.
* Confidentialité : la confidentialité d'un actif désigne sa capacité à être protégé contre l'accès non autorisé. Par exemple, pour l'imprimante Imprim20000, la confidentialité serait importante car si les données de l'imprimante sont accessibles à des tiers non autorisés, cela peut entraîner des violations de la vie privée et de la confidentialité des clients de l'entreprise.

En utilisant ces critères de disponibilité, intégrité et confidentialité, vous pouvez évaluer la valeur de chaque actif pour l'entreprise et déterminer l'impact sur la société en cas d'exécution d'un scénario à risque. Par exemple, si l'imprimante Imprim20000 est indisponible en raison d'une attaque informatique, cela peut entraîner des retards de production et des pertes financières pour l'entreprise. De même, si l'intégrité de l'imprimante est compromise en raison d'une erreur de logiciel, cela peut entraîner des pertes financières pour l'entreprise. Si la confidentialité de l'imprimante est compromise en raison d'une fuite de données, cela peut entraîner des violations de la vie privée et de la confidentialité des clients de l'entreprise, ce qui peut avoir un impact négatif sur la réputation de l'entreprise.

**Pour les actifs financiers,** la disponibilité consiste à s'assurer que les ressources financières de l'entreprise sont accessibles de manière fiable et à tout moment. La perte de disponibilité de ces actifs peut entraîner des retards ou des arrêts de production, ainsi que des pertes financières.

L'intégrité des actifs financiers consiste à s'assurer que ces ressources sont protégées contre les erreurs, les modifications non autorisées et les fraudes. La perte d'intégrité de ces actifs peut entraîner des erreurs de comptabilité et de reporting, ainsi que des pertes financières.

La confidentialité des actifs financiers consiste à s'assurer que ces ressources sont protégées contre l'accès non autorisé et la divulgation à des tiers. La perte de confidentialité de ces actifs peut entraîner des fuites d'informations sensibles et une perte de confiance de la part des clients et des partenaires.

Il est donc important de mettre en place des mesures de sécurité adéquates pour protéger la disponibilité, l'intégrité et la confidentialité des actifs financiers de l'entreprise.

Voici un résumé plus court des critères de sécurité pour les actifs financiers:

* Disponibilité: s'assurer que les ressources financières sont accessibles de manière fiable à tout moment.
* Intégrité: protéger les actifs financiers contre les erreurs, les modifications non autorisées et les fraudes.
* Confidentialité: protéger les actifs financiers contre l'accès non autorisé et la divulgation à des tiers.

**Pour les actifs immatériels,** la disponibilité consiste à s'assurer que ces éléments intangibles sont accessibles de manière fiable et à tout moment. La perte de disponibilité de ces actifs peut entraîner des retards ou des arrêts de production, ainsi que des pertes financières.

L'intégrité des actifs immatériels consiste à s'assurer que ces éléments sont protégés contre les erreurs, les modifications non autorisées et les fraudes. La perte d'intégrité de ces actifs peut entraîner des erreurs de comptabilité et de reporting, ainsi que des pertes financières.

La confidentialité des actifs immatériels consiste à s'assurer que ces éléments sont protégés contre l'accès non autorisé et la divulgation à des tiers. La perte de confidentialité de ces actifs peut entraîner des fuites d'informations sensibles et une perte de confiance de la part des clients et des partenaires.

Il est donc important de mettre en place des mesures de sécurité adéquates pour protéger la disponibilité, l'intégrité et la confidentialité des actifs immatériels de l'entreprise.

Voici un résumé plus court des critères de sécurité pour les actifs immatériels:

* Disponibilité: s'assurer que les éléments intangibles sont accessibles de manière fiable à tout moment.
* Intégrité: protéger les actifs immatériels contre les erreurs, les modifications non autorisées et les fraudes.
* Confidentialité: protéger les actifs immatériels contre l'accès non autorisé et la divulgation à des tiers.

**Pour les actifs matériels,** la disponibilité consiste à s'assurer que ces équipements, outils et installations sont accessibles de manière fiable et à tout moment. La perte de disponibilité de ces actifs peut entraîner des retards ou des arrêts de production, ainsi que des pertes financières.

L'intégrité des actifs matériels consiste à s'assurer que ces éléments sont protégés contre les erreurs, les modifications non autorisées et les dégradations. La perte d'intégrité de ces actifs peut entraîner des coûts de réparation et de maintenance supplémentaires, ainsi que des pertes financières.

La confidentialité des actifs matériels consiste à s'assurer que ces éléments sont protégés contre l'accès non autorisé et la divulgation à des tiers. La perte de confidentialité de ces actifs peut entraîner la divulgation d'informations sensibles et une perte de confiance de la part des clients et des partenaires.

Voici un résumé plus court des critères de sécurité pour les actifs matériels:

* Disponibilité: s'assurer que les équipements, outils et installations sont accessibles de manière fiable à tout moment.
* Intégrité: protéger les actifs matériels contre les erreurs, les modifications non autorisées et les dégradations.
* Confidentialité: protéger les actifs matériels contre l'accès non autorisé et la divulgation à des tiers.

**Pour les actifs humains,** la disponibilité consiste à s'assurer que les employés et les dirigeants de l'entreprise sont en mesure de remplir leurs fonctions de manière fiable et à tout moment. La perte de disponibilité de ces actifs peut entraîner des retards ou des arrêts de production, ainsi que des pertes financières.

L'intégrité des actifs humains consiste à s'assurer que ces employés et dirigeants sont loyaux et dignes de confiance, et qu'ils respectent les valeurs et les règles de l'entreprise. La perte d'intégrité de ces actifs peut entraîner une baisse de productivité, une perte de qualité et une perte de confiance de la part des clients et des partenaires.

La confidentialité des actifs humains consiste à s'assurer que les informations confidentielles de l'entreprise sont protégées contre la divulgation à des tiers par ces employés et dirigeants. La perte de confidentialité de ces actifs peut entraîner la divulgation d'informations sensibles et une perte de confiance de la part des clients et des partenaires.

Il est donc important de mettre en place des mesures de sécurité adéquates pour protéger la disponibilité, l'intégrité et la confidentialité des actifs humains de l'entreprise.

Voici un résumé plus court des critères de sécurité pour les actifs humains:

* Disponibilité: s'assurer que les employés et dirigeants de l'entreprise sont en mesure de remplir leurs fonctions de manière fiable à tout moment.
* Intégrité: protéger les actifs humains en veillant à ce qu'ils soient loyaux et dignes de confiance, et en faisant respecter les valeurs et les règles de l'entreprise.
* Confidentialité: protéger les actifs humains en veillant à ce que les informations confidentielles de l'entreprise ne soient pas divulguées à des tiers par ces employés et dirigeants.

Il est important de mettre en place des mesures de sécurité pour protéger ces actifs, afin d'éviter tout retard ou arrêt de production, toute baisse de productivité et de qualité, et toute fuite d'informations sensibles.

**Pour les actifs clients**, la disponibilité consiste à s'assurer que les informations et les services proposés à ces clients sont accessibles de manière fiable et à tout moment. La perte de disponibilité de ces actifs peut entraîner une perte de confiance de la part des clients et une baisse de leur fidélité.

L'intégrité des actifs clients consiste à s'assurer que les informations fournies à ces clients sont exactes et fiables, et que les services proposés sont de qualité. La perte d'intégrité de ces actifs peut entraîner une perte de confiance de la part des clients et une baisse de leur fidélité.

La confidentialité des actifs clients consiste à s'assurer que les informations confidentielles de ces clients sont protégées contre la divulgation à des tiers. La perte de confidentialité de ces actifs peut entraîner une perte de confiance de la part des clients et une baisse de leur fidélité.

Voici un résumé plus court des critères de sécurité pour les actifs clients:

* Disponibilité: s'assurer que les informations et services proposés à ces clients sont accessibles de manière fiable à tout moment.
* Intégrité: protéger les actifs clients en veillant à ce que les informations fournies soient exactes et fiables, et que les services proposés soient de qualité.
* Confidentialité: protéger les actifs clients en veillant à ce que les informations confidentielles de ces clients ne soient pas divulguées à des tiers.

Il est important de mettre en place des mesures de sécurité pour protéger ces actifs, afin de maintenir la confiance et la fidélité des clients de l'entreprise.

**Étape 3 : Identifier les menaces et les vulnérabilités associées aux actifs**

Voici un résumé plus court des menaces et vulnérabilités associées aux actifs financiers:

* Voles de données financières
* Fraudes financières
* Pertes de revenus
* Pertes de capital
* Pertes de valeur des actifs financiers

Voici quelques exemples de menaces et de vulnérabilités qui peuvent affecter les actifs financiers de l'entreprise:

* Les vols de données financières: cela peut se produire lorsque des tiers non autorisés accèdent aux systèmes informatiques de l'entreprise et récupèrent des informations financières sensibles.
* Les fraudes financières: cela peut se produire lorsque des employés ou des tiers malveillants utilisent frauduleusement les fonds de l'entreprise à des fins personnelles.
* Les pertes de revenus: cela peut se produire lorsque l'entreprise est incapable de facturer ses clients ou de percevoir des paiements en temps voulu.
* Les pertes de capital: cela peut se produire lorsque l'entreprise investit dans des projets qui échouent ou qui ont des rendements inférieurs aux attentes.
* Les pertes de valeur: cela peut se produire lorsque les actifs financiers de l'entreprise perdent de la valeur en raison de facteurs tels que l'inflation, la baisse des taux d'intérêt ou l'instabilité des marchés financiers.

Voici un résumé plus court des menaces et vulnérabilités associées aux actifs immatériels:

* Perte de la propriété intellectuelle
* Perte de la qualité de l'image de marque
* Perte de la confiance des clients
* Perte de la motivation et de l'engagement des employés
* Perte de la compétitivité

Voici quelques exemples de menaces et de vulnérabilités qui peuvent affecter les actifs immatériels de l'entreprise:

* La perte de la propriété intellectuelle: cela peut se produire lorsque des tiers utilisent sans autorisation les brevets, les marques, les licences ou les secrets commerciaux de l'entreprise.
* La perte de la qualité de l'image de marque: cela peut se produire lorsque l'entreprise est associée à des pratiques non éthiques ou non durables, ou lorsqu'elle est impliquée dans des litiges ou des controverses.
* La perte de la confiance des clients: cela peut se produire lorsque l'entreprise ne parvient pas à satisfaire les attentes de ses clients en termes de qualité, de service ou de sécurité.
* La perte de la motivation et de l'engagement des employés: cela peut se produire lorsque les employés de l'entreprise ne se sentent pas valorisés ou soutenus par leur employeur, ou lorsqu'ils ne partagent pas les valeurs et les objectifs de l'entreprise.
* La perte de la compétitivité: cela peut se produire lorsque l'entreprise est dépassée par ses concurrents en termes d'innovation, de qualité ou de prix.

Voici quelques exemples de menaces et de vulnérabilités qui peuvent affecter les actifs matériels de l'entreprise:

* Les vols ou les actes de vandalisme: cela peut se produire lorsque des tiers s'emparent illégalement des actifs matériels de l'entreprise ou les endommagent intentionnellement.
* Les défaillances ou les pannes: cela peut se produire lorsque les actifs matériels de l'entreprise tombent en panne ou ne fonctionnent plus de manière adéquate.
* Les incendies ou les catastrophes naturelles: cela peut se produire lorsque les actifs matériels de l'entreprise sont détruits par un incendie ou par des catastrophes naturelles telles que des inondations, des tempêtes ou des tremblements de terre.
* La dégradation ou l'obsolescence: cela peut se produire lorsque les actifs matériels de l'entreprise perdent de leur valeur ou de leur utilité en raison de l'usure ou de l'obsolescence.
* Les cyberattaques: cela peut se produire lorsque des tiers utilisent des techniques de piratage pour accéder ou contrôler à distance les actifs matériels de l'entreprise.

Voici un résumé plus court des menaces et vulnérabilités associées aux actifs humains:

* Perte de compétences et de savoir-faire
* Accidents de travail
* Harcèlement ou discriminations
* Conflits internes
* Mauvaise gestion de la santé mentale

Il est important de mettre en place des mesures de sécurité pour protéger les actifs humains contre ces menaces et vulnérabilités afin de préserver la santé et le bien-être des employés de l'entreprise et de garantir une productivité optimale.

Voici quelques exemples de menaces et de vulnérabilités qui peuvent affecter les actifs humains de l'entreprise:

* La perte de compétences et de savoir-faire: cela peut se produire lorsque les employés de l'entreprise quittent l'entreprise ou lorsque leur expertise n'est plus pertinente pour l'entreprise.
* Les accidents de travail: cela peut se produire lorsque les employés de l'entreprise sont victimes d'accidents de travail qui peuvent entraîner des pertes de productivité ou des coûts de soins de santé.
* Le harcèlement ou les discriminations: cela peut se produire lorsque les employés de l'entreprise sont victimes de harcèlement ou de discriminations, ce qui peut avoir un impact négatif sur leur motivation et leur bien-être.
* Les conflits internes: cela peut se produire lorsque les employés de l'entreprise sont en désaccord sur des sujets importants pour l'entreprise, ce qui peut entraîner des tensions et des pertes de productivité.
* La mauvaise gestion de la santé mentale: cela peut se produire lorsque les employés de l'entreprise souffrent de troubles mentaux ou de stress chronique et que l'entreprise ne met pas en place des mesures adéquates pour les soutenir.

Voici quelques exemples de menaces et de vulnérabilités qui peuvent affecter les actifs clients de l'entreprise:

* La perte de confiance des clients: cela peut se produire lorsque les clients de l'entreprise perdent confiance dans l'entreprise en raison de problèmes de qualité, de service ou de sécurité.
* La perte de la loyauté des clients: cela peut se produire lorsque les clients de l'entreprise sont tentés par les offres de concurrents ou lorsqu'ils ne se sentent pas satisfaits par leur relation avec l'entreprise.
* Les fuites de données ou les atteintes à la confidentialité: cela peut se produire lorsque les données des clients de l'entreprise sont divulguées à des tiers ou lorsque leur vie privée est compromise.
* Les litiges ou les controverses: cela peut se produire lorsque les clients de l'entreprise sont impliqués dans des litiges ou des controverses avec l'entreprise.
* Les problèmes de réputation: cela peut se produire lorsque l'entreprise est associée à des pratiques non éthiques ou non durables ou lorsqu'elle est impliquée dans des litiges ou des controverses qui peuvent nuire à sa réputation auprès de ses clients.

**Étape 4 : Présenter 2 scénarios de risques combinant les actifs, leurs menaces et leurs vulnérabilités. Identifier la vraisemblance de vos scénarios. (Choisir les scénarios de risque qui vous semblent les plus réalistes).**

Voici deux exemples de scénarios de risque combinant les actifs, les menaces et les vulnérabilités associées à l'imprimante industrielle Imprim20000 :

**Scénario 1** : Attaque de déni de service

Actifs : l'imprimante Imprim20000

Menace : déni de service (perturbation du fonctionnement de l'imprimante)

Vulnérabilité : faiblesse des mesures de protection contre les attaques de déni de service Vraisemblance : moyenne à élevée (les attaques de déni de service sont fréquentes et peuvent être facilement réalisées par des individus ou des groupes malveillants avec de faibles compétences techniques)

Impact : élevé (si l'imprimante est indisponible, cela peut entraîner des retards de production et des pertes financières pour l'entreprise)

**Scénario 2** : Fuite de données sensibles

Actifs : l'imprimante Imprim20000

Menace : divulgation d'informations (fuite de données sensibles de l'imprimante)

Vulnérabilité : absence de chiffrement des données de l'imprimante

Vraisemblance : moyenne à élevée (les fuites de données sont fréquentes et peuvent être causées

**Scénario 3 :**

Actifs: Actifs matériels (imprimantes industrielles)

Menace: Vols ou actes de vandalisme

Vulnérabilité: Absence de mesures de sécurité adéquates (systèmes de surveillance, verrous de sécurité, etc.)

Vraisemblance: Élevée - Les vols ou les actes de vandalisme sont des menaces courantes pour les actifs matériels et sont souvent facilités par des vulnérabilités telles que l'absence de mesures de sécurité adéquates.

**Scénario 4**:

Actifs: Actifs humains (employés)

Menace: Mauvaise gestion de la santé mentale

Vulnérabilité: Absence de programmes de soutien pour les employés souffrant de troubles mentaux ou de stress chronique

Vraisemblance: Élevée - La mauvaise gestion de la santé mentale des employés est un risque courant pour les entreprises et peut être exacerbé par des vulnérabilités telles que l'absence de programmes de soutien adéquats.

**Étape 5 : Réaliser une analyse de risque sur l’entreprise. (Basée sur le fichier Excel vu en cours)**

**Étape 6 : Réaliser une analyse de risque sur la nouvelle imprimante. (Basée sur le fichier Excel vu en cours)**

Calculer l’EPU (Espérance de Perte Unique) et l’EPA (Espérance de Perte Annuelle)

Pour calculer l'EPU (Espérance de Perte Unique) en cas de dysfonctionnement d'une imprimante, nous devons d'abord déterminer le coût moyen d'un incident. Pour ce faire, nous allons diviser le chiffre d'affaires moyen généré par jour par le nombre d'incidents moyens par an:

EPU = 35 000€ / 7 incidents/an = 5 000€/incident

Pour calculer l'EPA (Espérance de Perte Annuelle) en cas de dysfonctionnement d'une imprimante, nous allons multiplier l'EPU par le nombre d'incidents moyens par an:

EPA = EPU \* nombre d'incidents/an = 5 000€/incident \* 7 incidents/an = 35 000€/an

Pour calculer l'EPA avec la nouvelle imprimante qui permettra d'arriver à un TA (Taux d'Atténuation) de 85%, nous allons appliquer ce taux d'atténuation à l'EPA actuelle:

EPA avec nouvelle imprimante = EPA actuelle \* TA = 35 000€/an \* 0,85 = 29 750€/an

Le coût de la nouvelle imprimante est de 70 000€ par an, il est donc supérieur à l'EPA avec la nouvelle imprimante. Cela signifie qu'il pourrait être avantageux pour l'entreprise d'investir dans la nouvelle imprimante, car cela pourrait réduire les pertes annuelles liées aux incidents. Cependant, il convient de prendre en compte d'autres facteurs tels que les coûts initiaux d'acquisition et de maintenance de la nouvelle imprimante avant de prendre une décision définitive.

Calculer le ROSI de cette solution et les économies réalisées.

Pour calculer le ROSI (Return On Security Investment, ou taux de rentabilité de l'investissement en sécurité) de la nouvelle imprimante, nous allons devoir déterminer les économies réalisées en investissant dans cette solution. Pour ce faire, nous allons comparer l'EPA avec la nouvelle imprimante au coût de cette dernière:

Économies réalisées = coût de la nouvelle imprimante - EPA avec la nouvelle imprimante = 70 000€/an - 29 750€/an = 40 250€/an

Nous pouvons maintenant calculer le ROSI en divisant les économies réalisées par le coût de la nouvelle imprimante:

ROSI = économies réalisées / coût de la nouvelle imprimante = 40 250€/an / 70 000€/an = 0,57 ou 57%

Cela signifie que l'investissement dans la nouvelle imprimante génère un retour sur investissement de 57% chaque année.

**(1 pts) Étape 7 : Une échelle des priorités des actions est proposée par la direction. Proposez une échelle de charge de correction et proposer un planning projet afin de suivre la remédiation.**

Voici une échelle de charge de correction que vous pourriez proposer pour suivre la remédiation des actions identifiées dans l'analyse de risques :

1. Haute : les actions de cette catégorie doivent être corrigées immédiatement pour minimiser les risques pour l'entreprise.
2. Moyenne : les actions de cette catégorie doivent être corrigées dans un délai raisonnable, mais ne requièrent pas une attention immédiate.
3. Faible : les actions de cette catégorie sont importantes, mais leur correction peut être reportée sans causer de graves conséquences pour l'entreprise.

Voici un exemple de planning projet qui pourrait être utilisé pour suivre la remédiation des actions :

Étape 1 : identification des actions à remédier : réalisez une analyse de risques pour identifier toutes les actions qui nécessitent une remédiation.

Étape 2 : évaluation de la charge de correction : utilisez l'échelle de charge de correction décrite ci-dessus pour évaluer la charge de correction de chaque action.

Étape 3 : planification des actions de remédiation : en fonction de la charge de correction de chaque action, planifiez le moment et les ressources nécessaires pour remédier à chaque action.

Étape 4 : exécution des actions de remédiation : mettez en œuvre les plans d'action développés dans l'étape 3 pour remédier à chaque action.

Étape 5 : suivi et évaluation des progrès : suivez et évaluez les progrès réalisés dans la remédiation des actions pour s'assurer que toutes les actions ont été corrigées de manière adéquate.