Département de génie informatique et génie logiciel

INF8101

Analyse de cyberrisques

Projet Final

Soumis par

REDACTED (REDACTED)
REDACTED (REDACTED)
REDACTED (REDACTED)
REDACTED (REDACTED)
Diab Khanafer (REDACTED)
REDACTED (REDACTED)
REDACTED (REDACTED)

Soumis à

M^me^ Mikaela REDACTED

Automne 2023

6 décembre 2023

Table des matières

1. Introduction

LaForêt est une coopérative financière canadienne d'envergure qui offre multiples produits et services à ses membres d'un océan à l'autre. Son impact touche une part de marché significative. Elle emploie plus de 60 000 employés, dont 1000 qui sont dédiés uniquement à la cybersécurité, dans une économie et une atmosphère changeante où les risques en cybersécurité sont grandissants. En effet, selon la mise en contexte fournie par LaForêt, plusieurs incidents de cybersécurité surviennent chaque année, avec des coûts allant dans les millions de dollars canadiens.

Récemment, un incident de cybersécurité a poussé à la divulgation des données personnelles de 3200 membres de LaForêt. Dans ce contexte, la coopérative fait appel à notre firme de consultation afin de mettre en place une analyse qualitative et quantitative et prodiguer des recommandations. De plus, il s'agit de montrer l'intérêt des investissements en cybersécurité dans un contexte de grande entreprise.

2. Cyberrisque

Le cyberrisque qui est considéré en priorité dans les analyses qui suivront est celui de l'atteinte à la confidentialité des données de la coopérative LaForêt et de ses membres. La formulation de ce cyberrisque met en relief deux éléments capitaux. D'abord, évidemment, la confidentialité, puis surtout le mot « données », qui implique un accent mis sur les actifs informationnels plutôt que sur les conteneurs d'information.

3. Rôles et responsabilités

Pour faire face aux enjeux de cybersécurité, nous avons représenté les rôles et les responsabilités du personnel impliqué dans l'analyse du cyberrisque en utilisant une matrice RACI. Nous avons formé une équipe composée de membres internes de la coopérative LaForêt ainsi que de consultants externes pour nous épauler dans notre mission. Les rôles sont différenciés en ressources internes (bleu) et consultants (orange) (voir Tableau I.1 en annexe I). La matrice RACI est essentielle dans l'approche utilisée, puisqu'elle permet de différentier entre quatre niveaux de responsabilité que sont les suivants: « R » pour responsable, « A » pour approbateur , « C » pour consulter et finalement « I » pour informer.

4. Méthode d'analyse choisie

Pour notre analyse, nous avons pris la décision de faire usage de la méthode Octave Allegro. Cette décision vient de la raison que, selon notre cyberrisque choisi à la section 2 précédemment, nous faisons affaire à des actifs informationnels tels que les données de la coopération et de ces clients, ce qui est exactement ce sur quoi la logique d'Octave Allegro est axée.

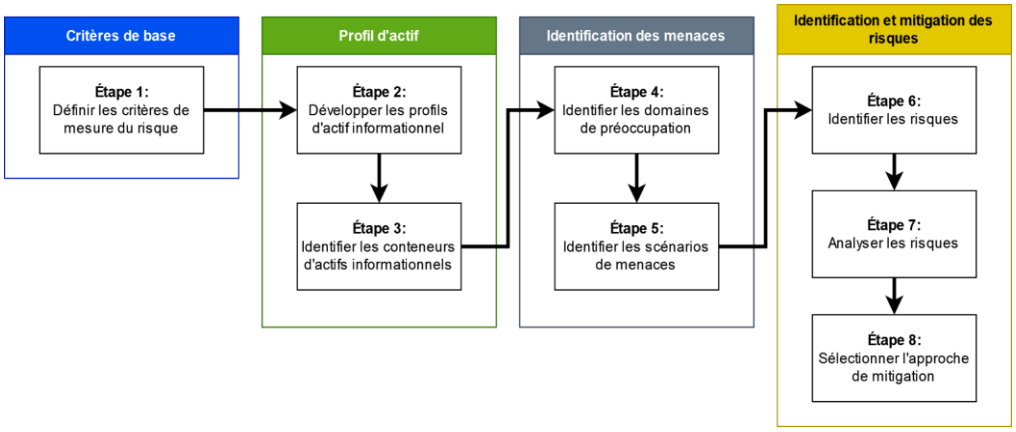

Figure 1. Schéma traduit de la méthode Octave Allegro [1]

5. Octave Allegro

Les sections suivantes détaillent chaque étape de la méthode d'analyse de risque qualitative Octave Allegro. Ces sections sont représentées sur la figure 1 ci-dessus.

5.1. Définir les critères de mesure du risque

Cette première étape permet d'établir les critères qui seront utilisés pour évaluer les effets d'un risque sur la mission et les objectifs de la coopérative. Elle sert aussi à hiérarchiser les domaines en fonction de leur importance pour l'organisation. Les zones d'impact sont les moteurs organisationnels qui font survivre l'entreprise en question. Après les avoir identifiées, elles sont présentées sous une échelle de 1 à 5 allant de la moins importante (1) à la plus importante (5) comme montré dans le tableau A.1. Dans le cas de LaForêt, l'analyse montre que la zone d'impact « Réputation et confiance des membres »est la plus importante alors que la zone « Santé et sécurité » est la moins importante parmi les cinq zones d'impact identifiées.

Par la suite, nous élaborons chacune des zones d'impacts identifiées en identifiant les niveaux de mesure de risque avec des cadrans faibles, modérés ou élevés (voir tableaux A.2 à A.6 dans l'annexe A). Le cadran faible a été identifié comme étant notre seuil d'acceptabilité du risque, et il sera utilisé pour continuer notre analyse.

5.2. Développer les profils d'actifs informationnels

La deuxième étape d'Octave Allegro vise à établir un profil complet des actifs informationnels de l'entreprise LaForêt. Dans une situation réelle, une coopérative financière aurait certainement des dizaines, voire des centaines d'actifs informationnels à protéger et à analyser.

Compte tenu de la lourdeur et du caractère très complet de la méthode d'analyse Octave Allegro, il a été convenu que seulement deux actifs informationnels seraient analysés ici. Ces deux actifs informationnels sont les suivants:

- Profil du membre de la coopérative (Tableau B.1)

- Code source de l'application mobile et artéfacts associés (Tableau B.2)

Pour chaque actif informationnel, Octave Allegro demande à renseigner plusieurs types d'information. D'abord, il faut spécifier le nom de l'actif et le raisonnement derrière sa criticité. Respectivement, cela correspond aux deux premières lignes des tableaux cités ci-dessus. Cela est essentiel pour bien en comprendre la pertinence. Ensuite, il faut décomposer l'actif informationnel en plusieurs composants informationnels, qui sont finalement les pièces d'information spécifiques qui constituent l'actif informationnel. Pour le profil du membre, on peut le décomposer en pensant au numéro d'assurance sociale, au prénom au nom… Les tableaux en annexe permettent de constater tous les détails.

Il faut ensuite indiquer le propriétaire de l'actif informationnel, puis expliquer en quoi chaque requis de sécurité[1] est important pour l'actif analysé. On termine l'analyse avec l'identification du requis de sécurité le plus important pour l'actif, dans le contexte de la coopérative. Pour le cas de cette analyse, l'intégrité a été considérée comme le requit le plus important pour chaque actif dû à la nature de l'organisation de la coopérative. Toutefois, notre analyse subséquente et nos conclusions se porteront davantage sur la confidentialité, puisqu'il s'agit du cyberrisque analysé.

5.3. Identifier les conteneurs d'actifs informationnels

L'identification des conteneurs, l'équivalent des **biens supports** dans la méthode EBIOS, est essentielle pour identifier les risques pesant sur l'actif informationnel. Les endroits où un actif informationnel est stocké, transporté ou traité peuvent devenir des points de vulnérabilité et des menaces qui mettent l'actif informationnel en danger. À l'inverse, ils peuvent également devenir des endroits où des contrôles peuvent être mis en œuvre pour garantir que les actifs informationnels soient protégés contre les dommages, afin qu'ils puissent être utilisés comme prévu [3]. Nous allons aborder ces contrôles dans l'étape 8 d'Octave Allegro.

Cette étape est réalisée en utilisant la feuille de travail de la Carte de l'Environnement de Risque, telle que décrite dans le tableau C.1 de l'annexe C. Les conteneurs se divisent en trois catégories : Technique, Physique et Personnes, ainsi que deux types d'espaces de stockage : Interne (à l'organisation) et Externe (sous contrôle d'entités externes sous-traitantes comme des fournisseurs).

En suivant ces catégories et types de contenants, nous pouvons donc identifier les conteneurs Physique et Personnes de nos actifs. (Tableaux C.1 à C.6 de l'annexe C)

5.4. Identifier les domaines de préoccupation

Cette étape commence le processus de l'identification des menaces. Ces domaines de préoccupation sont synonymes au facteur de risque de la méthode EBIOS. Ce sont des scénarios du

[1] Les requis de sécurité sont la confidentialité, l'intégrité et la disponibilité dans le cadre de cette analyse.

monde réel qui contribuent à la survenance d'un événement redoutable et/ou à la compromission de la sécurité d'un système.

Pour le premier actif , profil de membre de la coopérative, nous avons étudié les trois scénarios suivants :

- Apparition d'erreurs de saisie/mise à jour/impression de données de profil du membre de la coopérative effectuées par le personnel opérationnel.
- Ségrégation des rôles et privilèges qui n'aurait pas été effectuée de manière adéquate, laissant ainsi des trous (fromage suisse) dans la sécurité interne.
- Le bug/erreur contenu dans l'application qui apparaît lorsque le personnel informatique effectue le déploiement ou la maintenance.

Pour le deuxième actif, code source de l'application mobile et artéfacts associés, nous avons étudié les trois scénarios suivants :

- Mot de passe de la base de données en clair dans un répertoire public.
- Utilisation de la faille de sécurité de type "jour zéro" d'une application par l'interne/parties externes.
- Hameçonnage d'un employé de l'équipe de développement avec des accès au code source de l'application mobile.

5.5. Identifier les scénarios de menace

La cinquième étape nous permet de déterminer quels sont les scénarios de menaces. Cette étape nous permet de définir qui sont les acteurs potentiels, quels sont leurs motifs ainsi que les moyens qu'ils pourraient utiliser pour mener à terme leurs missions. Nous pouvons faire le parallèle avec les étapes 2 à 4 de EBIOS, où l'étape 2 met en valeur les sources de risque et leurs motivations, l'étape 3 consiste à cartographier les menaces et l'étape 4 qui permet de détailler le chemin d'attaque.

Une fois le scénario établi, nous évaluons la probabilité de chaque scénario de manière qualitative afin de nous permettre de les traiter par ordre de priorité dans les étapes suivantes. Dans le cadre de notre analyse qualitative, nous avons étudié six scénarios pour nos deux actifs informationnels . (Voir les tableaux de l'annexe E)

5.6. Identifier les risques

Cette étape vise à déterminer comment le scénario de menace qui a été enregistré dans chaque risque lié aux actifs informationnels peut avoir un impact sur la compagnie et ses diverses conséquences.

Nous avons deux tableaux pour chaque actif informationnel (profil de membre de la coopérative, code source de l'application mobile et les artéfacts associés, Annexe F.2) qui présente les scénarios de menaces et conséquences. On remarque que pour chaque menace, les conséquences

touchent majoritairement à la réputation, au légal et financier de la compagnie.

Le tableau de gravité (Annexe F.1) présente le niveau de gravité de chaque zone d'impacts ainsi que leur priorité (qui a été lors de l'étape 1). Pour comprendre ce tableau, nous avons utilisé un barème de 1 à 3 pour bas, moyen et haut et nous multiplions leur priorité par ce barème. Par exemple, la réputation et la confiance du client lorsque le risque est jugé haut, auraient un niveau de gravité de 15, car nous multiplions sa priorité (5) par le barème du risque haut (3).

5.7. Analyser les risques

Cette étape vise à déterminer comment le scénario de menace qui a été enregistré dans chaque risque lié aux actifs informationnels peut avoir un impact sur la compagnie et ses différentes conséquences. Pour le profil de membre de la coopérative et le code source de l'application mobile et artéfacts associés, nous avons trois tableaux (Annexe G.1 à G.6) qui sont trois sujets de préoccupation différents traité lors de l'étape 4 pour chacun de ces sujets, nous prenons en compte les impacts et appliquons notre table de gravité vue dans l'étape 6 pour ainsi pouvoir y attribuer un score de risque relatif qui va dépendre de la priorité de la zone d'impact pour le sujet en question ainsi que sa valeur qui est notre barème étant bas, moyen et haut. Ce score relatif est réparti sur une échelle de 0 à 45 comme on peut le voir au tableau H.1. Et avec ce score de risque relatif, nous attribuons une probabilité. Et comme ça avait été dit à l'étape 5, la probabilité aide une organisation à déterminer les scénarios les plus probables compte tenu de son environnement opérationnel unique.

5.8. Sélectionner une approche d'atténuation

Une fois les risques hiérarchisés, on passe à l'étape 8 qui représente la dernière étape du processus OCTAVE Allegro, des stratégies d'atténuation sont élaborées en tenant compte de la valeur de l'actif et de ses exigences de sécurité, des conteneurs dans lesquels il se trouve et de l'environnement opérationnel de l'organisation. Les risques devant être atténués sont choisis en fonction de leurs impacts et de leurs probabilités. Pour cela, il n'existe pas de voie décisive à suivre, il s'agira d'une décision des parties intéressées. Le traitement des risques reprend les quatre options que nous avons déjà détaillées auparavant, à savoir réduire, réduire ou transférer, transférer ou accepter, accepter les risques. Cette étape se compose de trois activités principales :

La première activité de l'étape 8 consiste simplement à trier chacun des risques identifiés selon leur score de risque et probabilité. Catégoriser les risques de manière ordonnée va aider à commencer à prendre des décisions sur leur statut d'atténuation. (Tableau H.1)

Dans la deuxième activité, il faut séparer les risques en quatre groupes: les risques ayant le score le plus élevé doivent se trouver dans le premier groupe, les risques les plus bas dans le quatrième groupe. (Tableau H.2)

L'activité 3 consiste à attribuer une approche d'atténuation à chacun des risques. Pour tous les profils de risque à atténuer, il faut développer une stratégie d'atténuation comme suit :

1. Noter le conteneur dans lequel le contrôle sera implémenté.
2. Décrivez les contrôles à mettre en œuvre et tout risque résiduel pour l'actif une fois le contrôle mis en œuvre.

En ce qui concerne l'étude du cas LaForêt, les stratégies d'atténuation des scénarios de préoccupation des deux actifs informationnels dans les étapes précédentes sont dans les annexes Tableau H.3 et Tableau H.4. L'élaboration de ses stratégies a été faite en s'assurant que la confidentialité des données de l'organisation et de ses clients ne soit pas atteinte.

L'étape 8 de la méthode OCTAVE Allegro se rapproche beaucoup avec l'atelier 5 de la méthode EBIOS et la comparaison entre les deux met en lumière les similitudes et les différences dans la gestion des risques.

Étape 8 de la méthode Octave Allegro:

- **Nature de l'étape :** L'étape 8 d'Octave Allegro se concentre sur l'élaboration de stratégies d'atténuation des risques identifiés.
- **Objectif :** L'objectif principal est de définir des approches spécifiques pour réduire, maintenir, refuser ou transférer les risques prioritaires.
- **Facteurs pris en compte :** Les stratégies d'atténuation sont formulées en prenant en compte la valeur de l'actif, les exigences de sécurité, les conteneurs, et l'environnement opérationnel de l'organisation.
- **Décision :** La sélection des risques à atténuer repose sur une décision collective des parties prenantes impliquées dans la gestion des risques.

Atelier 5 de la méthode EBIOS:

- **Nature de l'atelier :** L'atelier 5 d'EBIOS correspond à l'analyse des risques, où l'évaluation des scénarios de risques est réalisée.
- **Objectif :** L'objectif principal est d'évaluer les vulnérabilités, les menaces et les impacts associés aux actifs d'information et de proposer des mesures de sécurité.
- **Facteurs pris en compte :** L'analyse des risques dans EBIOS examine les mesures de prévention, de détection, de réaction, et les mesures organisationnelles en réponse aux scénarios de risques spécifiques.
- **Décision :** Les mesures de sécurité proposées sont généralement élaborées par consensus lors de réunions impliquant les parties prenantes.

Similitudes :

- Les deux méthodes visent à identifier des mesures spécifiques pour traiter les risques identifiés.
- Les deux approches reconnaissent l'importance de la participation des parties prenantes dans le processus de décision.

Différences :

- Les terminologies et la structure des deux méthodes diffèrent.
- Octave Allegro met l'accent sur la hiérarchisation des risques et la formulation de stratégies d'atténuation, tandis qu'EBIOS se concentre sur l'analyse des risques et la proposition de mesures de sécurité.
- Les types de mesures considérées peuvent varier entre les deux méthodes, bien que l'objectif global reste le même.

En résumé, bien que les étapes aient des noms différents et des approches spécifiques, elles partagent l'objectif fondamental de traiter les risques de manière proactive et de renforcer la sécurité de l'information au sein de l'organisation.

6. Analyse qualitative - Conclusion

En conclusion de notre analyse qualitative, il est indéniable que les menaces pesant sur la confidentialité des données de la coopérative LaForêt et de ses membres ont le potentiel d'impacter négativement notre réputation et la confiance de nos membres. Pour faire face à ces défis, nous avons formulé plusieurs recommandations stratégiques. Dans un premier temps, nous préconisons la réalisation de tests d'intrusions approfondis afin de déceler toute faille potentielle dans nos systèmes, garantissant ainsi une protection proactive contre d'éventuelles vulnérabilités. De plus, nous proposons la création d'une équipe de réponse aux incidents, assurant une réactivité accrue pour prévenir toute fuite de données et minimiser les conséquences d'éventuels incidents de sécurité. Par ailleurs, afin de renforcer notre conformité et de nous assurer que nos pratiques de sécurité sont à la hauteur des normes les plus strictes, nous recommandons le recours à des audits de sécurité externes. En incorporant ces recommandations, nous aspirons à renforcer significativement notre posture de sécurité, à anticiper les menaces futures et à assurer la sécurité, la confidentialité et la confiance de nos membres.

7. Méthode choisie - Analyse quantitative

L’analyse quantitative est une étape primordiale pour être mesure de mieux comprendre l’impact financier de la mise en place de différentes mesures de traitement du risque. Parmi les mesures identifiées à l’aide de la méthode d’analyse qualitative (Octave Allegro), il a fallu se concentrer sur certaines mesures spécifiques d’intérêt, notamment car ces mesures n’étaient pas déjà mises en place par la coopérative LaForêt.

La méthode d’analyse choisie est la méthode du ROSI, soit le *Return on Security Investment*. Cette méthode permet de constater, à l’aide de différents paramètres calculés, l’argent gagné ou perdu suite aux investissements faits du côté de la cybersécurité, notamment pour traiter un risque. Son fonctionnement se base d’abord sur la valeur des actifs à protéger, le potentiel de perte suite aux incidents, le ratio de mitigation des mesures en place et, bien sûr, leur coût. Les éléments d’intérêt et la formule utilisée pour les calculer sont présentés dans le tableau I.2 de l’annexe I. Essentiellement, il s’agit d’analyser la profitabilité financière des mesures de contrôle et de supporter la direction de la coopérative dans l’allocation des ressources financières.

8. ROSI

Avec les informations fournies par la coopérative, il a été difficile d'établir le ROSI, qui doit se baser sur des valeurs chiffrées. En effet, il a été nécessaire de se baser sur des moyennes prises de diverses sources afin d'estimer le coût moyen d'un incident de cybersécurité ainsi que la fréquence de ceux-ci dans le cadre d'une grande entreprise. Après des recherches, le coût moyen d'un seul incident de cybersécurité est établi à 6,75 millions de dollars CAD [8]. De plus, la fréquence moyenne est, elle, établie à 25 incidents d'envergures variables par an [7].

À l'aide de ces deux informations, il est maintenant possible d'estimer la valeur du ALE, l'espérance de perte annualisée. La multiplication nous présente un ALE estimé de 169 millions de dollars CAD par année. Pour calculer le ROSI, il convient ensuite de trouver le ratio de mitigation et le coût total de nos solutions. Les sous-sections suivantes décrivent les coûts estimés pour six solutions proposées et la manière dont les estimations ont été calculées, puis il sera possible de calculer le ROSI avec des hypothèses sur les ratios de mitigation.

8.1. Tests d'intrusion de base

Chaque type de service devrait subir des tests d'intrusion annuels de base (pas nécessairement un exercice de *Red Team*. Nous avons, avec notre expérience professionnelle, estimé qu'un tel test pourrait être facturé 150$ par heure pour environ 400 heures de travail pour une entreprise comme LaForêt. Cela représente un coût annuel de 60 000$.

8.2. Sauvegardes régulières

Les sauvegardes régulières sont importantes et devraient suivre le principe 3-2-1, c'est-à-dire 3 copies de sauvegardes sur 2 médias différents avec 1 copie physiquement déplacée dans un autre lieu que le lieu de la sauvegarde. Cette méthode peut considérer que les sauvegardes font déjà partie des coûts d'opération normaux. Il a été estimé que ce coût peut se concevoir comme le salaire d'une équipe dédiée à l'application des meilleures configurations et l'identification des solutions de sauvegarde défaillantes. Un budget de 1 million de dollars serait alloué à cette équipe. [5]

8.3. Réponse aux incidents

Avoir une équipe dédiée à la réponse aux incidents serait important pour assurer une réponse rapide et ne pas dépendre d'une firme externe spécialisée pour une réponse initiale. Il est estimé que 20 employés au salaire de 150 000 dollars annuellement permettraient de combler ce besoin pour un total de 3 000 000 de dollars. Un budget d'un million supplémentaire serait prévu pour un accompagnement par une firme externe spécialisée. Cela porte le total de cette mesure à 4 millions de dollars.

8.4. Audits de sécurité et certifications

Une recherche a permis de déterminer que le coût d'une certification de sécurité comme ISO2700X aurait un coût approximatif de 100 000 $ pour une entreprise de la taille de LaForêt [6, 7]. Puisque le renouvellement doit avoir lieu chaque 3 ans, le coût annuel de la mesure est estimé à environ 34 000 dollars. Cette mesure permettrait d'identifier des brèches que les tests d'intrusion n'auraient pu identifier ainsi que renforcer le suivi des pratiques recommandées par le standard choisi.

8.5. Contrôle des accès physiques

Cela peut se traduire par l'installation d'un système de gestion des accès avec badges pour quatre points d'entrée par succursale. Le fait que 500 succursales soient concernées pour un total de 65 000 employés avec des badges au coût de 10$ chacun permet d'établir d'abord 650 000$ pour les badges, puis un coût pour l'installation physique de 2 750$ par point d'entrée pour une somme de 5 500 000$ [11]. Le total de la mesure est donc de 6 150 000$, mais un remplacement estimé tous les 10 ans permet d'assumer un coût réel annuel de 615 000$ pour cette mesure.

8.6. Révision annuelle des accès à l'information

Cette révision est essentielle pour jongler avec les départs et les promotions d'employés afin de s'assurer qu'ils n'aient les accès que pour ce qu'ils doivent effectivement utiliser au quotidien. Il s'agit aussi de s'assurer que les actions nécessitant des droits d'administration soient faites avec des comptes séparés. On peut estimer ce coût comme une tâche qu'une équipe de 10 employés doit faire une fois par année et que cela s'intègre à leur travail existant. Pour 800 heures-personnes à 50$ par heure, cette mesure est estimée à 40 000 dollars.

8.7. Calcul du ROSI

Il est donc finalement possible de calculer le ROSI. Le coût total des mesures est de 5 749 000 dollars. En choisissant un ratio de mitigation conservateur de 40% pour l'ensemble des mesures, le ROSI est égal à 10,76, ce qui indique qu'au sauve plus de 10 fois l'argent investi. Même en supposant que le ratio de mitigation serait aussi mince que 10%, le ROSI serait égal à 1,93: on sauve presque le double de l'argent qu'on aura investi.

9. Conclusion en lien avec le cyberrisque

À la lumière des résultats de l'analyse qualitative et de l'analyse quantitative, il est évident qu'investir en sécurité est primordial, et que cela ne doit pas être considéré comme une dépense ou une contrainte. LaForêt devrait rapidement mettre en place les mesures suggérées par l'analyse Octave Allegro qu'elle n'a pas déjà mise en place, et peut se fier sur l'estimation quantitative faite avec ROSI pour se conforter dans le caractère responsable des dépenses qui seront engagées.

Spécifiquement en lien avec notre cyberrisque, LaForêt peut être confiante dans l'analyse utilisant Octave Allegro, car elle se focalise sur les données plutôt que sur les conteneurs. Les mesures concrètes présentées dans le ROSI sont des mesures permettant d'améliorer la sécurité des actifs informationnels et, par extension, leur confidentialité.

10. Pistes de réflexion

Cette section permet une perspective d'ouverture sur les questions suivantes. D'abord, quelles sont les menaces et les attaques les plus courantes pour chaque secteur d'affaires? Ensuite, les risques présentés s'alignent-ils sur les tendances de l'industrie ? Enfin, comment protéger la réputation et les valeurs de l'organisation ?

Le Centre Canadien pour la Cybersécurité publie régulièrement un rapport évaluant les cybermenaces auxquelles font face les individus, les organisations et surtout les fournisseurs d'infrastructures critiques - l'Évaluation des cybermenaces nationales (ECMN) [4]. Assurer la sécurité de ces fournisseurs est essentiel, car ils englobent les secteurs d'affaires fondamentaux à la société et à l'économie. On parle entre autres de l'agriculture, de la construction, de la santé, de l'énergie, du transport et bien sûr de la finance.

L'ECMN souligne qu'avec les enjeux géopolitiques accrus, ces secteurs sont "les cibles de cyberactivités malveillantes cautionnées par des [États-nations]" [4] et surtout la cible de cybercriminels indépendants utilisant des attaques de rançongiciels par intérêt financier. En effet, les infrastructures essentielles étendent leur exposition au risque avec des technologies opérationnelles de plus en plus connectées à l'Internet. Aussi, ces cybercriminels savent qu'un temps d'arrêt dans ces secteurs est critique, donc que ces fournisseurs sont plus enclins à payer rapidement [4].

L'industrie financière, elle, est exposée au même risque de rançongiciels que les secteurs d'affaires, ainsi qu'à d'autres risques spécifiques à ce secteur. Les fuites de données liées aux menaces internes et aux attaques par phishing, étant les plus communes [12]. Cela s'aligne avec notre travail qui fait ressortir les cybercriminels comme les acteurs de risques clés avec comme résultat principal la divulgation d'informations confidentielles.

Il est possible, quoique difficile, de protéger la réputation et les valeurs d'une organisation dans le cadre d'un incident de cybersécurité, mais cela nécessite une grande préparation en amont. En effet, des plans de communication clairs doivent être établis, et il est important de tenir les utilisateurs impactés au courant des développements dès que possible. Une approche par obscurantisme ne peut qu'aliéner et décevoir les utilisateurs. De plus, l'accent du message doit être mis dans les mesures en place et les mesures correctives qui seront appliquées pour prévenir d'autres incidents dans l'avenir.

11. Références

La liste ci-dessous présente les références utilisées pour produire cette analyse.

[1] Presses Cisco. (2017). Formal Risk Analysis Structures: OCTAVE and FAIR. Disponible : https://www.ciscopress.com/articles/article.asp?p=2803867&seqNum=4 (consulté le: 27 novembre 2023)

[2] Januanto, Ari & Febria, Dede & Suroso, Jarot. (2018). Risk Management of Debtor Information System (At Bank XYZ Using OCTAVE Allegro Method).

[3] Woody, C. Applying OCTAVE: Practitioners Report (CMU/SEI-2006-TN-010, ADA448425). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006. Disponible : http://www.sei.cmu.edu/publications/documents/06.reports/06tn010.html (consulté le: 27 novembre 2023)

[4] Centre Canadien pour la Cybersécurité. (28 octobre 2022). "Évaluation des cybermenaces nationales 2023-2024," Gouvernement du Canada, Disponible : https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024 (consulté le: 2 décembre 2023).

[5] Modern data analytics in banking: Benefits, outlook & more. (2023). Hitachi Solutions. Disponible: https://global.hitachi-solutions.com/blog/big-data-banking/ (consulté le: 24 novembre 2023)

[6] *Build trust. unlock growth.* (Sans date). *Secureframe*. Disponible : https://secureframe.com/hub/soc-2/audit-cost (consulté le: 26 novembre 2023).

[7] Laval, R., & Laval, R. (20 octobre 2023). 25 incidents de cybersécurité par année chez les grosses entreprises. Courrier Laval. Disponible : https://courrierlaval.com/25-incidents-cybersecurite-par-annee-grosses-entreprises-canada/ (consulté le: 26 novembre 2023)

[8] Amanda Stephenson La Presse Canadienne. (28 juillet 2021). Cyberattaques: Coût record pour les entreprises canadiennes. LaPresse. Disponible : https://www.lapresse.ca/affaires/techno/2021-07-28/cyberattaques/cout-record-pour-les-entreprises-canadiennes.php (consulté le: 22 novembre 2023)

[9] Magnusson, A. (2023) How to maintain ISO 27001 certification in 2023 and beyond, StrongDM. Disponible : https://www.strongdm.com/blog/how-to-maintain-iso-27001-certification (consulté le: 24 novembre 2023).

[10] R. Caralli, J. Stevens, L. Young, and W. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," *Carnegie Mellon University, Software Engineering Institute's Digital Library*. Software Engineering Institute, Technical Report CMU/SEI-2007-TR-012, 1-May-2007. Disponible : https://doi.org/10.1184/R1/6574790.v1. (consulté le: 22 novembre 2023).

[11] Kistler, K. (2023) *The Ultimate Guide to Badge Entry Systems for Access Control*, *ButterflyMX® - Official Site | Video Intercoms & Access Control*. Disponible : https://butterflymx.com/blog/badge-entry-system/ (consulté le: 26 novembre 2023).

[12] Bouveret, A. (2018) *Cyber risk for the financial sector: A Framework for Quantitative Assessment*, *IMF*. Disponible : https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924 (consulté le: 2 décembre 2023).

Annexe A

Tableau A.1: Priorité des zones d'impact

Priorité	Zone d'impact
5 (plus importante)	Réputation/Confiance des membres
4	Financier
3	Amendes/Sanctions légales
2	Productivité
1 (moins importante)	Santé et sécurité

Feuille de travail Allegro	Réputation et confiance des clients		
Impact	Faible	Modéré	Élevé
Réputation	La réputation est très peu affectée.	La réputation est pas mal affectée, des efforts sont nécessaires pour l'améliorer.	La réputation est affectée sévèrement, c'est presque irréparable.
Perte de clients	Diminution de moins de 2% de la clientèle due à un manque de confiance.	Perte de 2% à 10% des clients dus à un manque de confiance.	Diminution de plus de 10% de la clientèle due à un manque de confiance.

Tableau A.2: Zone d'impact - Réputation et confiance des clients

Tableau A.3: Zone d'impact - Financier

Feuille de travail Allegro	Financier		
Impact	Faible	Modéré	Élevé
Financier	Les coûts financiers sont minimes. Les pertes financières sont limitées et peuvent être gérées sans difficulté. Pas plus que 2% du chiffre d'affaires annuel.	Les coûts financiers sont significatifs, mais gérables. Ils ont un impact sur les résultats financiers de l'organisation, mais ne sont pas catastrophiques. Entre 2% et 5% du chiffre d'affaires annuel.	Les coûts financiers sont élevés. Ils ont un impact important sur les résultats financiers de l'organisation et peuvent nuire à sa stabilité financière. Plus de 5% du chiffre d'affaires annuel

Feuille de travail Allegro	Sanctions légales		
Impact	Faible	Modéré	Élevé
Sanctions	Les sanctions légales sont mineures et n'ont qu'un impact limité sur l'organisation. Les coûts juridiques sont gérables et ne représentent pas une menace majeure.	Les sanctions légales sont significatives, mais encore gérables. Elles ont un impact notable sur le budget de l'organisation et peuvent nécessiter des ressources juridiques substantielles.	Les sanctions légales sont très élevées. Elles ont un impact grave sur les finances de l'organisation, menaçant potentiellement sa stabilité financière et sa réputation.

Tableau A.4: Zone d'impact - Sanctions légales

Tableau A.5: Zone d'impact - Productivité

Feuille de travail Allegro	Productivité		
Impact	Faible	Modéré	Élevé
Productivité	La productivité de l'organisation est légèrement affectée. Les perturbations sont mineures, et il y a peu d'incidence sur la capacité de l'organisation à maintenir ses opérations.	La productivité de l'organisation est significativement affectée. Il y a des interruptions dans les opérations, et des efforts supplémentaires sont nécessaires pour maintenir un niveau de productivité acceptable.	La productivité de l'organisation est gravement affectée. Les interruptions sont majeures, et il peut être difficile de maintenir des niveaux de productivité acceptables, ce qui peut entraîner des retards importants.

Feuille de travail Allegro	Santé et sécurité		
Impact	Faible	Modéré	Élevé
Santé et sécurité	L'impact sur la santé et la sécurité est mineur. Les risques pour la santé et la sécurité des employés et des parties prenantes sont limités, et les incidents ont peu de conséquences.	L'impact sur la santé et la sécurité est significatif. Il y a des risques pour la santé et la sécurité des employés et des parties prenantes, et des mesures doivent être prises pour réduire ces risques.	L'impact sur la santé et la sécurité est grave. Il y a des risques sérieux pour la santé et la sécurité des employés et des parties prenantes, et des mesures immédiates sont nécessaires pour atténuer ces risques.

Tableau A.6: Zone d’impact - Santé et sécurité

Annexe B

Tableau B.1: Actif informationnel du profil de membre

Actif critique	**Profil de membre de la coopérative financière**	
Raisonnement (Pourquoi cet actif est-il particulièrement important?)	Le profil des membres de la banque est d'importance cruciale, car il contient diverses données sensibles et personnelles. Les clients sont essentiels à l'entreprise, car elle ne peut pas fonctionner sans eux et qu'ils constituent sa principale source de revenus. En considérant les risques réputationnels qu'un incident de sécurité causerait, les membres seraient susceptibles de déserter l'entreprise, lui portant alors un coup fatal.	
Description (Quels sont les composants informationnels de cet actif critique?)	Le profil du membre contient les données suivantes : numéro d'assurance sociale, adresse, nom, prénom, numéro de téléphone, profil d'investisseur, tendances de retrait et de dépôt, types de comptes, limites des comptes, forfaits des comptes, informations bancaires, spécimen de chèque, employeur, salaire annuel.	
Propriétaire (Qui possède cet actif critique?)	Département des services bancaires aux particuliers	
Requis de la sécurité (Quels sont les requis de la sécurité pour l'actif critique?)	C	L'information d'un membre ne devrait pouvoir être consultée que par lui-même et les conseillers de la banque. Il faut se protéger contre les accès non autorisés. Certaines informations du profil de membre ne sont pas non plus accessibles au membre.
	I	L'exactitude de l'information est primordiale pour permettre de prendre des décisions sur le dossier bancaire et envoyer de la publicité ciblée efficace. Ces décisions peuvent avoir un effet conséquent sur la vie du membre et ne doivent absolument pas être prises sur la base d'informations erronées ou falsifiées.
	A	L'indisponibilité momentanée des informations n'est pas souhaitable, sans être critique. Une disponibilité permanente sans possibilité de récupération serait critique.
Requis de la sécurité le plus important (C/I/A)	**Intégrité** Raison: Dû aux répercussions à long terme sur la vie financière des membres, l'intégrité est le requis de sécurité le plus important.	

Tableau B.2: Actif informationnel du code source

Actif critique	**Code source de l'application mobile et artéfacts associés**	
Raisonnement (Pourquoi cet actif est-il particulièrement important?)	Cet actif ne doit pas être public dans la mesure où la banque conserve une propriété intellectuelle sur les programmes qu'elle produit. Dans une optique où le produit n'est pas à source ouverte, il peut contenir différents secrets et/ou clés d'accès qui permettraient à un attaquant de pivoter. L'aspect de protection des innovations face aux compétiteurs de la coopérative est aussi particulièrement important.	
Description (Quels sont les composants informationnels de cet actif critique?)	Dans cet actif, on retrouve notamment les composants informationnels suivants: langage de programmation utilisé, modules tiers utilisés, plugiciels, cadriciels, informations d'authentification tel que des clés d'API, base de données locales, informations de développement (clés d'API, jetons d'authentification), documents d'architecture logicielle.	
Propriétaire (Qui possède cet actif critique?)	Département des technologies de l'information	
Requis de la sécurité (Quels sont les requis de la sécurité pour l'actif critique?)	C	Protéger le vol de propriété intellectuelle et les artéfacts de développement pouvant permettre à un attaquant de pivoter. Empêcher la rétro-ingénierie de la solution mobile bancaire.
	I	Un attaquant qui gagnerait un accès en modification au code source pourrait le modifier et y intégrer le code de son choix afin de perpétrer des attaques ultérieures.
	A	Il n'y a pas vraiment d'enjeu de disponibilité autrement que par des modifications d'intégrité spécifiques.
Requis de la sécurité le plus important (C/I/A)	**Intégrité** Raison: Dû aux répercussions à long terme sur l'introduction de logiciels espions ou de portes dérobées, l'intégrité est le requis de sécurité le plus important, bien que la confidentialité suive de très près.	

Annexe C

Tableau C.1: Carte de l'environnement de Risque (Technique)-Profil du membre

Profil de membre de la coopérative	
Carte de l'environnement de risque des actifs informationnels (Technique)	
Interne	
Description du conteneur	**Propriétaire(s)**
Base de données Le profile du membre est stocké dans une base de données	Data Center (Centre de données)
Application du système bancaire de base Le profil du membre est utilisé pour créer des solutions adaptées aux clients de la coopérative.	Équipe de développement
Externe	
Description du conteneur	**Propriétaire(s)**
Application Web LaForêt Le profile de membre peut être accédé et changer à travers l'application	Équipe de développement

Profil de membre de la coopérative	
Carte de l'environnement de risque des actifs informationnels (Physique)	
Interne	
Description du conteneur	**Propriétaire(s)**
Documents de profil du membre liés à la soumission et l'allocation de crédit	Équipe de prêt
Rapports imprimés relatifs à besoins internes	Équipe administrative, Équipe de prêt

Tableau C.2: Carte de l'environnement de Risque (Physique)-Profil du membre

Tableau C.3: Carte de l'environnement de Risque (Personnes)-Profil du membre

Profil de membre de la coopérative	
Carte de l'environnement de risque des actifs informationnels (Personnes)	
Interne	
Description du conteneur	**Propriétaire(s)**
Personnel de développement informatique	Personnel de développement informatique
Personnel Juridique	Équipe Juridique
Externe	
Description du conteneur	**Propriétaire(s)**
Membre de la coopérative	Membre de la coopérative

Tableau C.4: Carte de l'environnement de Risque (Technique)- Code source

Code source de l'application mobile et artéfacts associés	
Carte de l'environnement de risque des actifs informationnels (Technique)	
Interne	
Description du conteneur	**Propriétaire(s)**
Logiciel de gestion de versions décentralisé	Data Center (Centre de données)
Bibliothèque tierce utilisée dans le code source	Équipe de développement
Base de données Stockage de données technique	Data Center (Centre de données)

Code source de l’application mobile et artéfacts associés	
Carte de l’environnement de risque des actifs informationnels (Physique)	
Interne	
Description du conteneur	**Propriétaire(s)**
Serveur physique	Centre de données physique
Ordinateur de bureau, portable	Département Informatique

Tableau C.5:Carte de l'environnement de Risque (Physique)-Code source

Code source de l’application mobile et artéfacts associés	
Carte de l’environnement de risque des actifs informationnels (Personnes)	
Interne	
Description du conteneur	**Propriétaire(s)**
Personnel de développement informatique	Personnel de développement informatique

Tableau C.6: Carte de l'environnement de Risque (Personnes)-Code source

Annexe D

Tableau D.1: Sujet de préoccupation - Profil de membre de la coopérative

Profil de membre de la coopérative	
No	Sujet de préoccupation
1	L'apparition d'erreurs de saisie/mise à jour/impression de données de profil du membre de la coopérative effectuées par le personnel opérationnel.
2	Ségrégation des rôles et privilèges qui n'aurait pas été effectuée de manière adéquate, laissant ainsi des trous (fromage suisse) dans la sécurité interne.
3	Le bug/erreur contenu dans l'application qui apparaît lorsque le personnel informatique effectue le déploiement ou la maintenance.

Tableau D.2: Sujet de préoccupation - Code source de l'application mobile et artéfacts associés

Code source de l'application mobile et artéfacts associés	
No	Sujet de préoccupation
1	Mot de passe de la base de données en clair dans un répertoire public.
2	Utilisation de la faille de sécurité de type "jour zéro" d'une application par l'interne/parties externes.
3	Hameçonnage d'un employé de l'équipe de développement avec des accès au code.

Annexe E

Tableau E.1: Scénario de menace 1

Sujet de préoccupation	**L'apparition d'erreurs de saisie/mise à jour/impression de données de profil du membre de la coopérative effectuées par le personnel opérationnel.**			
Propriétés de la menace				
Acteur	Moyens	Motif	Résultat	Probabilité
Personnel opérationnel	Le personnel utilise les services bancaires de base pour effectuer les opérations financières.	Une erreur s'est produite en raison d'une erreur humaine (Accidentel)	Modification; Interruption.	Modérée
		Volontaire	Divulgation; Modification; Perte; Interruption.	

Tableau E.2: Scénario de menace 2

Sujet de préoccupation	**Ségrégation des rôles et privilèges qui n'aurait pas été effectuée de manière adéquate, laissant ainsi des trous (fromage suisse) dans la sécurité interne.**			
Propriétés de la menace				
Acteur	Moyens	Motif	Résultat	Probabilité
Menace interne	L'employé malveillant exploite ses privilèges existants pour accéder aux applications contenant les profils des membres de la coopérative.	Motivé par des intentions malveillantes, l'employé pourrait vendre les informations confidentielles des membres à des tiers ou les utiliser à des fins de chantage. (Volontaire)	Les informations sensibles des membres sont compromises, ce qui peut entraîner des pertes financières, une perte de confiance des membres, voire des litiges juridiques. (Divulgation)	Modérée, dépendant des contrôles d'accès et de la surveillance en place.
Attaquant externe (MPA)	Exploitation de vulnérabilités dans le système pour contourner les contrôles d'accès et accéder aux applications.	Vol d'informations sensibles pour des gains financiers ou pour mener des attaques ultérieures, telles que la fraude ou le vol d'identité.	Accès non autorisé aux profils des membres, compromettant la confidentialité des informations.	Dépendante des mesures de sécurité en place, mais peut être modérée.

Erreur humaine	Un employé peut accidentellement accorder des droits d'accès inappropriés lors de la gestion des autorisations.	Manque de formation, précipitation, ou négligence dans la gestion des autorisations.	Accès non autorisé aux profils des membres, compromettant la confidentialité des informations.	Élevée si les processus de gestion des autorisations ne sont pas rigoureusement suivis.

Tableau E.3: Scénario de menace 3

Sujet de préoccupation	**Le bug/erreur contenu dans l'application qui apparaît lorsque le personnel informatique effectue le déploiement ou la maintenance.**			
Propriétés de la menace				
Acteur	Moyens	Motif	Résultat	Probabilité
Employé négligent	L'employé informatique peut négliger les procédures de déploiement, sauter des étapes de vérification, ou introduire des modifications non testées.	Manque de compréhension, précipitation, ou négligence dans l'exécution des tâches.	Introduction de bugs ou d'erreurs dans l'application en production. (Modification; Interruption.)	Faible à élevée en fonction du niveau de rigueur dans les procédures internes.
Attaquant externe exploitant la vulnérabilité nouvellement introduite	Identifiant la faille introduite lors du déploiement, un attaquant peut exploiter cette vulnérabilité pour accéder à des données sensibles ou perturber le fonctionnement de l'application.	Vol de données, sabotage, ou autre activité malveillante.	Exploitation réussie de la vulnérabilité introduite, compromettant la sécurité de l'application.	Dépendante de la visibilité et de la détection de la vulnérabilité par les équipes de sécurité.
Concurrent malveillant	Un concurrent peut essayer d'introduire délibérément des bugs dans l'application pendant son déploiement, dans le but de discréditer la solution concurrente.	Gain concurrentiel, déstabilisation du marché.	Présence de bugs intentionnels dans l'application, impactant la confiance des utilisateurs.	Modérée, dépendante de la compétitivité du marché et des enjeux.

Tableau E.4: Scénario de menace 4

Sujet de préoccupation	**Mot de passe de la base de données en clair dans un répertoire public.**			
Propriétés de la menace				
Acteur	Moyens	Motif	Résultat	Probabilité
Cybercriminel	Un attaquant peut utiliser des outils pour scanner les répertoires publics de l'entreprise.	Vol de données, chantage, sabotage, ou autres motivations malveillantes.	Accès non autorisé à la base de données, modification de données, ou perturbation des services.	Modérée(Moyenne), dépendante des contrôles d'accès et des mesures de surveillance en place.

Tableau E.5: Scénario de menace 5

Sujet de préoccupation	**Utilisation de la faille de sécurité de type "jour zéro" d'une application par l'interne/parties externes.**			
Propriétés de la menace				
Acteur	Moyens	Motif	Résultat	Probabilité
Cybercriminel	Reconnaissance pour obtenir de l'information sur les technologies utilisées. Exploitation d'une faille dans le logiciel.	Vol de données, chantage, sabotage, ou autres motivations malveillantes.	Accès non autorisé à des données sensibles, modification de données, ou perturbation des services.	Élevée si les vulnérabilités ne sont pas rapidement corrigées et si la surveillance est insuffisante

Tableau E.6: Scénario de menace 6

Sujet de préoccupation	**Hameçonnage d'un employé de l'équipe de développement avec des accès au code source de l'application mobile.**			
Propriétés de la menace				
Acteur	Moyens	Motif	Résultat	Probabilité

Cybercriminel	L'attaquant utilise les réseaux sociaux pour trouver un développeur et ses intérêts.	Revente du code source aux compétiteurs (Volontaire).	Divulgation.	Modérée/Moyenne

Annexe F

Tableau F.1: Échelle de Gravité

Zones d'impacts	**Priorité**	Bas	Moyen	Haut
Réputation et confiance du client	**5**	5	10	15
Financière	**4**	4	8	12
Amendes et sanctions légales	**3**	3	6	9
Productivité	**2**	2	4	6
Sécurité et santé	**1**	1	2	3

Tableau F.2: de scénario de menaces et conséquences

Scénario de menaces	Conséquences
Profil de membre de la coopérative	
L'apparition d'erreurs de saisie/mise à jour/impression de données de profil du membre de la coopérative effectuées par le personnel opérationnel.	Impacts sur les erreurs de déclaration aux régulateurs qui entraînent des amendes, mais nécessitent également du temps supplémentaire pour réenregistrer et corriger les erreurs. 1. Réputation 2. Légal 3. Financière
Ségrégation des rôles et privilèges qui n'aurait pas été effectuée de manière adéquate, laissant ainsi des trous (fromage suisse) dans la sécurité interne.	1. Impact financier, réputation endommagée, perte de confiance des membres. 2. Risque financier, atteinte à la réputation, perturbation des opérations. 3. Pertes financières, violation de la confidentialité, diminution de la confiance des membres.

Le bug/erreur contenu dans l'application qui apparaît lorsque le personnel informatique effectue le déploiement ou la maintenance.	1. Perturbation des services, insatisfaction des utilisateurs, risque financier. 2. Risque financier, atteinte à la réputation, perte de confiance des utilisateurs. 3. Perte de clients, diminution de la part de marché, atteinte à la réputation.
Code source de l'application mobile et artéfacts associés	
Mot de passe de la base de données en clair dans un répertoire public	1. Impact financier, réputation endommagée, perte de confiance des membres. 2. Risque financier, atteinte à la réputation, perturbation des opérations. 3. Pertes financières, violation de la confidentialité, diminution de la confiance des membres.
Utilisation de la faille de sécurité de type "jour zéro" d'une application par l'interne/parties externes.	1. Impact financier 2. Atteinte à la réputation 3. Perturbation des opérations.
Hameçonnage d'un employé de l'équipe de développement avec des accès au code.	1. Impact financier 2. Atteinte à la réputation 3. Perturbation des opérations.

Annexe G

Tableau G.1

Profil de membre de la coopérative				
Sujet de préoccupation	Risque			
L'apparition d'erreurs de saisie/mise à jour/impression de données de profil du membre de la coopérative effectuées par le personnel opérationnel.	Gravité	Zone d'impact	Valeur	Score
		Réputation et confiance du client (5)	Moyen(2)	10
		Financière (4)	Bas(1)	4
		Amendes et sanctions légales (3)	Haut(3)	9
		Productivité (2)	Haut(3)	6
		Sécurité et santé (1)	Bas(1)	1
		Score de risque relatif		**30**
	Probabilité (étape 5)	**Modérée**		

Tableau G.2

Profil de membre de la coopérative				
Sujet de préoccupation	Risque			
Ségrégation des rôles et privilèges qui n'aurait pas été effectuée de manière adéquate, laissant ainsi des trous (fromage suisse) dans la sécurité interne.	Gravité	Zone d'impact	Valeur	Score
		Réputation et confiance du client (5)	Haut(3)	15
		Financière (4)	Moyen(2)	8
		Amendes et sanctions légales (3)	Moyen(2)	6

		Productivité (2)	Bas(1)	2
		Sécurité et santé (1)	Bas(1)	1
		Score de risque relatif		**32**
	Probabilité (étape 5)	**Modérée/Moyenne**		

Tableau G.3

Profil de membre de la coopérative				
Sujet de préoccupation	Risque			
Le bug/erreur contenu dans l'application qui apparaît lorsque le personnel informatique effectue le déploiement ou la maintenance.	Gravité	Zone d'impact	Valeur	Score
		Réputation et confiance du client (5)	Haut(2)	10
		Financière (4)	Moyen(2)	8
		Amendes et sanctions légales (3)	Bas(2)	6
		Productivité (2)	Bas(2)	4
		Sécurité et santé (1)	Bas(2)	2
		Score de risque relatif		**30**
	Probabilité (étape 5)	**Faible/Improbable**		

Tableau G.4

Code source de l'application mobile et artéfacts associés				
Sujet de préoccupation	Risque			
Mot de passe de	Gravité	Zone d'impact	Valeur	Score

la base de données en clair dans un répertoire public		Réputation et confiance du client (5)	Haut(3)	**15**
		Financière(4)	Haut(3)	**12**
		Amendes et sanctions légales(3)	Moyen(2)	**6**
		Productivité(2)	Bas(1)	**2**
		Sécurité et santé(1)	Bas(1)	**1**
		Score de risque relatif		**36**
	Probabilité (étape 5)	**Modérée/Moyenne**		

Tableau G.5

Code source de l'application mobile et artéfacts associés				
Sujet de préoccupation	Risque			
Utilisation de la faille de sécurité de type "jour zéro" d'une application par l'interne/parties externes.	Gravité	Zone d'impact	Valeur	Score
		Réputation et confiance du client (5)	Haut (3)	**15**
		Financière(4)	Haut (3)	**12**
		Amendes et sanctions légales(3)	Moyen(2)	**6**
		Productivité(2)	Bas(1)	**2**
		Sécurité et santé(1)	Bas(1)	**1**
		Score de risque relatif		**36**
	Probabilité (étape 5)	**Probable/Élevée**		

Tableau G.6

Code source de l'application mobile et artéfacts associés				
Sujet de préoccupation	Risque			
Hameçonnage d'un employé de l'équipe de développement avec des accès au code	Gravité	Zone d'impact	Valeur	Score
		Réputation et confiance du client (5)	Haut(3)	**15**
		Financière(4)	Haut(3)	**12**
		Amendes et sanctions légales(3)	Moyen(2)	**6**
		Productivité(2)	Bas(1)	**2**
		Sécurité et santé(1)	Bas(1)	**1**
		Score de risque relatif		**36**
	Probabilité (étape 5)	**Modérée/Moyenne**		

Remarques : Les scores générés dans cette activité sont uniquement destinés à être utilisés comme outil de priorisation. Les différences entre les scores de risque ne sont pas considérées comme pertinentes. En d'autres termes, un score de 48 signifie que le risque est relativement plus important pour l'organisation qu'un score de 25, mais la différence de 13 points n'a aucune importance.

Annexe H

Tableau H.1: Matrice de risque relative

Matrice de risque relative			
Probabilité	Score de Risque		
	30 à 45	16 à 29	0 à 15
Très probable	Groupe 1	Groupe 1	Groupe 2
Probable	Groupe 1	Groupe 2	Groupe 3
Modérée	Groupe 2	Groupe 3	Groupe 4
Improbable	Groupe 3	Groupe 4	Groupe 4

Tableau H.2: Approche de mitigation

Groupe	Approche de mitigation
Groupe 1	Réduire
Groupe 2	Réduire ou Transférer
Groupe 3	Transférer ou Accepter
Groupe 4	Accepter

Tableau H.3: Stratégie d'atténuation des risques pour le premier actif

Risk Mitigation	
Sujet de préoccupation	L'apparition d'erreurs de saisie/mise à jour/impression de données de profil du membre de la coopérative effectuées par le personnel opérationnel.
Approche de mitigation	Groupe 2: **Réduire ou transférer**
Sur quel conteneur appliqueriez-vous des contrôles ?(étape 3)	Quels contrôles administratifs, techniques et physiques appliqueriez-vous sur ce conteneur ? Quel risque résiduel serait encore accepté par l'organisation ?
Base de données	- Gestion des droits d'accès pour s'assurer que seuls les utilisateurs autorisés ont

	accès aux données et aux fonctionnalités nécessaires - Journalisation des activités - Audit des bases de données
Application du système bancaire de base	- Validation des entrées - Formation du personnel sur l'utilisation du système bancaire et les procédures appropriées pour éviter les erreurs.
Application Web LaForêt	- Contrôles d'accès basés sur les rôles - Journalisation des activités
Sujet de préoccupation	Ségrégation des rôles et privilèges qui n'aurait pas été effectuée de manière adéquate, laissant ainsi des trous (fromage suisse) dans la sécurité interne.
Approche de mitigation	Groupe 2: **Réduire ou transférer**
Sur quel conteneur appliqueriez-vous des contrôles ?(étape 3)	Quels contrôles administratifs, techniques et physiques appliqueriez-vous sur ce conteneur ? Quel risque résiduel serait encore accepté par l'organisation ?
Application du Système Bancaire de Base	- Séparation des tâches, de manière à ce que les utilisateurs aient accès uniquement aux fonctionnalités nécessaires pour leur rôle spécifique. - Contrôles d'accès basés sur les rôles pour restreindre l'accès aux fonctionnalités critiques et aux données des profils des membres.
Personnel de Développement Informatique & Centre de Données Informatiques	- Contrôles d'accès aux environnements de développement pour s'assurer que seuls les développeurs autorisés peuvent accéder aux données sensibles. - Journalisation des activités de développement, en particulier celles impliquant des données sensibles, pour une traçabilité accrue.
Personnel Juridique	- Sensibilisation à la confidentialité : Fournir une formation spécifique au personnel juridique sur la confidentialité des données des profils des membres et sur les procédures appropriées.

	- Contrôles d'accès aux données juridiques en fonction des besoins spécifiques du personnel juridique.
Membre de la Coopérative	- Mettre en place un portail en libre-service sécurisé qui permet aux membres d'accéder à leurs propres profils de manière sécurisée, réduisant la nécessité d'interventions du personnel.
Sujet de préoccupation	Le bug/erreur contenu dans l'application qui apparaît lorsque le personnel informatique effectue le déploiement ou la maintenance.
Approche de mitigation	Groupe 3: **Transférer ou Accepter**
Sur quel conteneur appliqueriez-vous des contrôles ? (étape 3)	Quels contrôles administratifs, techniques et physiques appliqueriez-vous sur ce conteneur ? Quel risque résiduel serait encore accepté par l'organisation ?
Base de Données	- Effectuez des sauvegardes régulières de la base de données avant toute opération de déploiement ou de maintenance. Cela permet de restaurer rapidement les données en cas de problème. - Testez régulièrement la procédure de restauration à partir des sauvegardes pour vous assurer qu'elle est fonctionnelle en cas de besoin.
Application du Système Bancaire de Base	- Utilisez des environnements de test dédiés pour évaluer les mises à jour ou les modifications avant de les déployer dans l'environnement de production. - Élaborez des procédures de réversion claires pour annuler rapidement les changements en cas de découverte d'un bug après le déploiement.
Application Web LaForêt	- Déployez les mises à jour de manière progressive, en commençant par un petit pourcentage d'utilisateurs, pour détecter et corriger rapidement les erreurs éventuelles. - Mettez en place des outils de surveillance en temps réel pour détecter les problèmes dès qu'ils surviennent, ce qui permet une réponse rapide.

Personnel de Développement Informatique & Centre de Données Informatiques	- Élaborez un plan de déploiement détaillé qui inclut des vérifications et des tests approfondis avant le déploiement dans l'environnement de production. - Assurez une formation continue du personnel informatique sur les meilleures pratiques de déploiement et de maintenance pour réduire les risques d'erreurs.

Tableau H.4: Stratégie d'atténuation des risques pour le deuxième actif

Risk Mitigation	
Sujet de préoccupation	Mot de passe de la base de données en clair dans un répertoire public
Approche de mitigation	Groupe 2: **Réduire ou Transférer**
Sur quel conteneur appliqueriez-vous des contrôles ?(étape 3)	Quels contrôles administratifs, techniques et physiques appliqueriez-vous sur ce conteneur ? Quel risque résiduel serait encore accepté par l'organisation ?
Code Source	- Privatiser le répertoire - Réviser les 'commits' régulièrement - Audit de sécurité
Base de données	- Sauvegarde régulière - Contrôle d'accès
Personnel de développement informatique & Centre de Données informatiques	- Chiffrement des mots de passe - Stockez les configurations sensibles, y compris les mots de passe, en dehors des répertoires publics. Utilisez des fichiers de configuration sécurisés avec des autorisations d'accès appropriées. - Politiques de mots de passe forts
Sujet de préoccupation	Utilisation de la faille de sécurité de type "jour zéro" d'une application par l'interne/parties externes.
Approche de mitigation	Groupe 1: **Réduire**
Sur quel conteneur appliqueriez-vous des contrôles ?(étape 3)	Quels contrôles administratifs, techniques et physiques appliqueriez-vous sur ce conteneur ? Quel risque résiduel serait encore accepté par l'organisation ?

Code source	- Analyse et test de sécurité - Programmation sécurisée - DevSecOps
Logiciel de gestion de versions décentralisé	- Mise à jour régulière du logiciel
Bibliothèque tierce utilisée dans le code source	- Mise à jour et patching des bibliothèques et dépendances externes dans le code source
Base de données Stockage de données techniques	- Chiffrement des données et du stockage - Politiques de rétention des données - Audit des bases de données - Mise à jour régulière
Serveur physique	- Contrôles d'accès physiques
Sujet de préoccupation	Hameçonnage d'un employé de l'équipe de développement avec des accès au code.
Approche de mitigation	Groupe 2: **Réduire ou transférer**
Sur quel conteneur appliqueriez-vous des contrôles ? (étape 3)	Quels contrôles administratifs, techniques et physiques appliqueriez-vous sur ce conteneur ? Quel risque résiduel serait encore accepté par l'organisation ?
Personnel de développement informatique	- Sensibilisation à la sécurité - Exercices de simulation d'hameçonnage - Activer MFA au compte du personnel
Ordinateur de bureau et portable	- Politiques de sécurité des courriels - Logiciel de sécurité (anti-virus…) - Mise à jour régulière - Limiter les privilèges

Annexe I

Tableau I.1 : Matrice RACI

Activités	Rôles						
	Directeur Général	Directeur Technique	RSSI	Gestionnaire SSI	Consultante en Gouvernance	Consultant de lutte contre fraude	Consultante en GR
	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED

Définir le cadre de la GR	A	A	R	I	I	I	C
Préparer les critères de base	A	R	C	I	C	I	I
Identifier les actifs informationnels	I	A	R	C	I	I	I
Identifier les menaces	I	I	A	R	I	I	I
Identifier les risques	I	I	A	R	I	I	I
Sélectionner des contrôles	I	A	R	r	I	I	I
Évaluer les risques	I	A	R	C	r	r	r
Choix de la méthode du traitement des risques	I	A	R	r	C	C	C
Élaborer un plan d'action	A	R	C	C	C	C	C

Remarques : Les "r" indiquent que ces individus ont un rôle de support ou de responsabilité pour un ensemble de sous-tâches pour une activité.

Tableau I.2 Éléments de calcul nécessaires pour l'analyse quantitative ROSI.

Élément	Formule
SLE (Espérance de perte unique)	Déterminé par une moyenne, voir section 8.
ARO (Taux d'occurrence annuel)	Déterminé par une moyenne, voir section 8.
ALE (Espérance de perte annualisée)	SLE * ARO
ROSI (Retour sur l'investissement en sécurité)	(ALE * Ratio de mitigation - Coût de la solution) / Coût de la solution