

POLITIQUE

SECURITÉ DES SYSTÈMES D'INFORMATIONS

Mise à jour : 3.13.26

1. Introduction

I. Objet du document

Ce document, intitulé « **Politique de Sécurité des Systèmes d'Informations** » (PSSI), fixe les principes fondateurs à l'égard de la sécurité des systèmes d'informations de Covea Finance, garants de la cohérence des actions et de la pérennité des investissements correspondants.

Les systèmes d'information recouvrent notamment :

- ✓ L'ensemble des informations (et les différents moyens et ressources de gestion associés) nécessaires au plein exercice des métiers et missions de Covea Finance ;
- ✓ Les informations sensibles confiées par les clients ou par les prestataires / partenaires avec lesquels Covea Finance est en relation, dont l'altération ou la divulgation pourrait porter atteinte à son image de marque, nuire aux intérêts des tiers concernés, voire entraîner des poursuites judiciaires ;
- ✓ Le patrimoine intellectuel de Covea Finance, composé de toutes les informations concourant à son savoir et son savoir-faire ;
- ✓ Les informations à caractère personnel relatives à ses collaborateurs.

Ce document souligne les principaux risques liés aux systèmes d'information auxquels Covea Finance doit faire face et expose plus particulièrement :

- ✓ Les obligations à respecter et principes de sécurité majeurs à appliquer ;
- ✓ Les principes de gouvernance à adopter à l'égard de la maîtrise de ces risques.

Il est complété par un ensemble de **procédures** déclinant les règles générales de sécurité SI applicables au sein de Covea Finance, l'ensemble constituant son **cadre de sécurité SI**.

II. Domaine d'application

Le cadre de sécurité SI s'applique à l'ensemble des moyens humains, techniques et organisationnels permettant de créer, de conserver, d'échanger et de partager des informations entre les acteurs internes et externes à Covea Finance, quelle que soit la forme sous laquelle elles sont exploitées (électronique, imprimée, manuscrite, vocale, image …) et en particulier :

- ✓ À l'ensemble du personnel autorisé à gérer des informations ou à utiliser, au niveau fonctionnel ou technique, des ressources des systèmes d'information de Covea Finance ;
- ✓ De manière contractuelle :

- A l'ensemble des prestataires et fournisseurs dès lors que, sur leurs périmètres d'intervention :
  - Ils utilisent les systèmes d'information de Covea Finance ;
  - Ils fournissent des services informatiques en nuage (Cloud) ;
  - Leur propre système d'information est relié au réseau informatique de Covea Finance ;
  - Ils hébergent une partie des systèmes d'information de Covea Finance ;
  - A l'ensemble des clients de Covéa Finance dès lors qu'ils effectuent des opérations au travers de ses systèmes d'informations ;

- A l'ensemble des partenaires de Covea Finance dès lors qu'ils effectuent des opérations au travers de ses systèmes d'information ;
  - ✓ À tous les composants matériels et logiciels des systèmes d'information support des activités de Covea Finance ;
  - ✓ Aux bâtiments / locaux abritant les ressources humaines et moyens informatiques de Covea Finance ;
  - ✓ À l'ensemble des procédures et modes opératoires de production et d'échange d'informations, quelle qu'en soit la nature (données, voix, images).

Toute entreprise ou organisme tiers qui doit interfacer ses systèmes d'information avec ceux de Covea Finance doit faire l'objet d'une analyse de risques permettant de préciser les conditions du raccordement dans le cadre d'un plan d'assurance sécurité respectant les principes de sécurité de Covea Finance.

III. Documentation de référence

- ✓ Politique Globale de Sécurité des Systèmes d'Information du groupe Covea
- ✓ Ensemble des recommandations des organismes de tutelle de Covéa Finance (AFG, AMF, ESMA)

2. Enjeux majeurs et objectifs de sécurité

I. Contexte

L'activité de Covéa Finance suit une approche de maitrise de ses risques afin de sécuriser ses opérations. A ce titre, garantir la sécurité et la conformité de ses systèmes d'informations constitue donc pour Covea Finance un enjeu clé dans un contexte où :

- ✓ L'évolution du système d'information est nécessaire pour répondre aux enjeux stratégiques de Covéa Finance

C2 - Interne

- ✓ Le risque lié aux cyber-attaques s'intensifie fortement du fait de la généralisation du télétravail et des architectures informatiques en nuage (Cloud) ;
- ✓ La France et l'Union Européenne, notamment, se dotent de lois et de règlements contraignants.

II. Enjeux majeurs des SI gérés par Covéa Finance

Les principaux enjeux de la sécurité des Systèmes d'Information s'inscrivent dans la volonté de Covea Finance :

- ✓ D'assurer la disponibilité de ses informations et la continuité des infrastructures et services informatiques ;
- ✓ De protéger l'ensemble de son patrimoine informationnel contre les menaces internes / externes et d'éviter en particulier le vol de données sensibles, notamment celles à caractère personnel ;
- ✓ De permettre l'évolution du système d'information de manière sécurisé pour les services délivrés par ses métiers ;
- ✓ De se conformer aux lois, règlementations et exigences contractuelles ;
- ✓ D'établir un climat de confiance permanent, tant en interne vis-à-vis de ses collaborateurs qu'en externe vis-à-vis des clients, fournisseurs et partenaires.

Face à de tels enjeux, puisque tout dysfonctionnement d'ampleur des systèmes d'information de Covea Finance peut ainsi conduire à :

- ✓ Une dégradation significative de la qualité du service, pouvant remettre en cause ses engagements contractuels, susceptible de porter atteinte durablement à son image de marque et entraîner :
  - • Un manque à gagner remettant en cause sa capacité de croissance et d'amélioration de son offre de services ;
  - • Une dégradation de sa compétitivité ;
  - • Une perte de crédibilité auprès de ses clients et ses partenaires ;
- ✓ Des pertes financières (perte de C.A., amendes / pénalités, détournements …) occasionnées notamment par :
  - • Le non-respect d'obligations contractuelles vis-à-vis de ses clients et partenaires ;
  - • Le vol de données sensibles confiées par ses clients et partenaires ;
  - • Des pertes de recours potentiels dans le cadre de litiges ;

• Des malversations ou fraudes favorisées par des faiblesses éventuelles des dispositifs de sécurité et de contrôle interne relatifs aux systèmes d'information ;

- ✓ La désorganisation d'une ou plusieurs activités clés engendrant notamment une dégradation du service, des pertes de productivité, l'accumulation de retards, l'accroissement des réclamations et litiges ;
- ✓ Un manquement à des obligations légales ou réglementaires susceptible d'engager la responsabilité civile, voire pénale, de Covea Finance, de ses dirigeants ou de ses salariés, notamment en cas de :

• Non-respect de la réglementation tutélaire ;

• Protection insuffisante de la confidentialité des informations à caractère personnel concernant notamment ses collaborateurs, clients, partenaires ;

• Non-respect des règles et principes relatifs au contrôle interne et à la gestion des risques applicables aux sociétés de gestion de portefeuille édictés par les autorités de tutelle ;

• D'usage frauduleux ou illégal des systèmes d'information.

III. Objectifs de sécurité des Systèmes d'Informations

Face à de tels enjeux, les objectifs de sécurité des Systèmes d'Informations de Covea Finance s'articulent autour de cinq axes majeurs :

- ✓ La performance et la sécurité des opérations d'une société de gestion de portefeuille ;
- ✓ L'existence de pistes d'audit et de dispositifs de contrôle ;
- ✓ La capacité de l'organisation à détecter un incident, à l'expliquer et à en fournir une preuve juridique ;
- ✓ La continuité d'activité ;
- ✓ La protection du patrimoine informationnel.

1. Performance et sécurité des opérations de gestion de portefeuille

La capacité de Covéa Finance à fournir des services de qualité est fondamentale pour assurer la protection des actifs financiers qui lui sont confiés. Ses systèmes d'information doivent donc :

- ➢ Assurer un traitement efficace et rigoureux des informations et des opérations liées à chacune de ses activités ;
- ➢ Fournir les dispositifs permettant de garantir :

• L'exécution des contrats et des obligations correspondantes ;

• La fourniture des services proposés ;

• L'exactitude et l'intégrité des informations manipulées ;

• La confidentialité des informations sensibles, internes ou confiées par un tiers ;

• La conformité des activités avec la législation et la réglementation (SGP en particulier).

2. Existence de pistes d'audit et de dispositifs de contrôle

Les conditions d'enregistrement, de conservation, de traitement des informations doivent règlementairement permettre une reconstitution aisée des opérations effectuées dans le cadre des activités de Covéa Finance. En outre, les systèmes d'informations doivent intégrer les dispositifs de contrôle nécessaires à la maîtrise des opérations qu'ils génèrent et à la justification des informations produites.

3. Détection des incidents et preuve

Face aux risques induits par la multiplication et l'interconnexion des systèmes d'information, l'identification, la qualification et l'explication d'un incident, voire la capacité à fournir des éléments de preuve s'avèrent particulièrement délicats.

Les systèmes d'informations doivent fournir les mécanismes permettant :

- De détecter tout incident ;
- D'en expliquer les raisons et d'orienter le choix des mesures correctives ;
- D'apporter, le cas échéant, la preuve juridique qu'un événement ou une opération présente un caractère frauduleux ou malveillant.

4. Continuité d'activité

Au regard de la criticité des opérations de Covéa Finance et des exigences règlementaires, la continuité d'activité est un élément essentiel pour une société de gestion de portefeuille.

La résilience opérationnelle numérique désigne la capacité d'une entité financière à anticiper, à se préparer, à réagir et à se remettre des perturbations qui pourraient avoir une incidence sur la fourniture de ses produits et services de base.

A ce titre, Covéa finance s'engage à :

- Mettre en place un calendrier de tests de continuité et de résilience adaptés ;

- Intégrer une segmentation précise des réseaux dans les plans de continuité et de gestion de crise.

Les systèmes d'informations doivent fournir les mécanismes permettant :

- La continuité d'activité des systèmes d'informations sur lesquels reposent les activités critiques ;
- De maintenir et réexaminer régulièrement un programme de tests de continuité d'activité faisant partie intégrante du dispositif de gestion des risques.

5. Protection du patrimoine informationnel

Au regard de la sensibilité des données manipulées, la protection du patrimoine informationnel de Covéa Finance est un pilier fondamental.

Les systèmes d'informations doivent fournir les mécanismes permettant :

- La classification des informations selon leur niveau de criticité ;
- Le chiffrement des informations secrètes ;

3. Obligations liées aux systèmes d'informations

I. Obligations légales et réglementaires

Covea Finance, en tant que personne morale, doit s'assurer tout particulièrement :

- ✓ Que ses activités se déroulent dans le respect des lois et règlements qui leur sont applicables ;
- ✓ Qu'elle respecte les exigences réglementaires qui lui sont applicables (RG AMF, RGDP, Directives AIFM, DORA, MIF, OPCVM, le code monétaire et financier, Orientations de L'ESMA relatives à la sous-traitance à des prestataires de services en nuage) en matière de sécurité des systèmes d'information ;
- ✓ Qu'elle a la capacité de répondre aux requêtes émanant des autorités judiciaires relatives au comportement de ses collaborateurs, notamment lors de l'usage des ressources de ses systèmes d'informations, et de fournir, le cas échéant, les preuves juridiques qu'un événement ou une opération présentent un caractère frauduleux ou malveillant ;

A ce titre, Covea Finance s'engage à :

- ✓ Déployer les actions de sensibilisation et formation réguliers sur les risques de cybersécurité. Les actions de sensibilisation et de formation seront adaptées en fonction du profil et des différents niveaux de responsabilité ;
- ✓ Préciser les sanctions applicables en cas de manquement ;

- ✓ Echanger au travers du groupe Covea et de ses filiales sur les aspects cyber en partageant les informations et les bonnes pratiques dans le domaine ;
- ✓ Se réserver le droit, à tout moment, d'effectuer les vérifications nécessaires dans le respect des obligations réglementaires et d'appliquer les sanctions définies ;
- ✓ Interrompre la relation avec un partenaire qui représenterait un risque pour le système d'information ou sa souveraineté ;
- ✓ Notifier les incidents majeurs aux autorités compétentes. Le RSSI transmettra sans délais les incidents impactant les activités critiques de Covéa Finance au RCCI conformément à la procédure définie ;
- ✓ Mettre en œuvre un programme de tests avancés dans le cadre de résilience numérique (ex. tests de pénétration fondés sur la menace) ;
- ✓ Mettre à jour la stratégie de continuité et de résilience qui sera validée par le CODIR ;
- ✓ Tenir un registre central des incidents impactant les activités critiques de Covéa Finance conformément à la procédure de gestion des incidents ;
- ✓ Élaborer une liste complète des actifs TIC* et de leurs interconnexions, incluant les prestataires ;
- ✓ Maintenir un registre pour suivre les incidents majeurs et consigner les actions correctives entreprises ;
- ✓ Organiser une formation régulière spécifique pour la direction sur les risques TIC* et leurs impacts.

*Technologie d'Information et de Communication.

De son côté, chaque utilisateur des systèmes d'information de Covea Finance doit respecter la législation applicable.

II. Comportements

Covea Finance a élaboré

• Une **Charte d'utilisation des systèmes d'informations** (Annexée au règlement intérieur) précisant les comportements à adopter dans le cadre de l'utilisation des ressources du système d'information mises à disposition des collaborateurs de Covea Finance.

• Une **Charte administrateur** précisant les droits et devoirs des administrateurs, et les règles de déontologie et de sécurité à suivre. Dans les cas où elle est annexée au règlement intérieur, une information des collaborateurs concernés doit être réalisée, son non-respect étant susceptible d'engager la responsabilité professionnelle et/ou pénale du contrevenant.

4. Rôles et responsabilités

I. Principes d'organisation

L'organisation de Covea Finance à l'égard de la protection de son patrimoine informationnel n'est pas uniquement l'affaire de spécialistes en sécurité. Elle relève de la responsabilité de chaque collaborateur, comme de celle de l'ensemble des échelons hiérarchiques, dans le respect des principes de séparation des pouvoirs.

1. Le rôle du collaborateur

La sécurité est essentiellement une affaire de responsabilités individuelles. Chaque collaborateur doit avoir la volonté d'acquérir les réflexes et les connaissances lui permettant d'adopter un comportement de vigilance à l'égard des risques inhérents à ses activités, d'appliquer les règles et les procédures de sécurité édictées et de rapporter tout incident ou anomalie constatée.

2. Le rôle de la hiérarchie

Chaque responsable doit contribuer à l'appréciation des risques dans son domaine d'activité et veiller à ce que les mesures permettant de les limiter soient intégrées aux processus opérationnels dont il a la charge.

II. Métier

Chaque métier est impliqué :

- ✓ Dans l'identification des risques liés aux systèmes d'information et de la mise en œuvre des moyens permettant de s'en prémunir ou d'en limiter les impacts éventuels à un seuil acceptable ;
- ✓ De la déclinaison et de l'application opérationnelle du cadre de sécurité SI sur son périmètre de responsabilité.

Sur son périmètre de responsabilité, elle s'assure :

- ✓ De la définition du niveau de sensibilité des informations manipulées et des processus de gestion associés ;
- ✓ De la définition des objectifs de sécurité (cf. § 2.III) que doivent respecter les systèmes d'informations support de ses activités, de manière permanente ou dans le cadre de nouveaux projets ;
- ✓ De l'intégration des règles et principes issus du cadre de sécurité SI dans les processus opérationnels et les processus projet ;
- ✓ Du respect, par ses équipes, des règles issues des directives et des dispositifs de sécurité organisationnels / techniques mis en place, notamment en matière de droits d'accès aux SI ;
- ✓ De la sensibilisation de ses équipes à la sécurité des systèmes d'informations ;
- ✓ Selon les procédures prévues, de la remontée des incidents de sécurité.

Enfin, chaque métier est force de proposition auprès du COMEX pour toute évolution du cadre de sécurité SI.

III. Pôle Système d'informations

Le Pôle SI étant lui-même un métier, il a sur l'ensemble de son périmètre de responsabilité, les mêmes obligations que celles décrites au § II ci-dessus.

Sur le périmètre des systèmes d'informations, la spécificité des missions assurées impose des responsabilités particulières inhérentes aux deux grandes natures d'activité couvertes :

- A1 : Des activités de pilotage de la production informatique permettant, par le recours à des technologies, infrastructures et processus opérationnels optimisés, de proposer aux métiers des systèmes d'information performants ;

- A2 : Des activités liées à des projets d'évolution des systèmes d'information du Groupe comprenant notamment :

    - Des activités d'étude et de conseil auprès des métiers ;
    - Des activités de gestion de projets pour le compte des métiers ;
    - Des activités de conception/optimisation, réalisation, livraison et maintenance de solutions applicatives ou techniques ;

1. Périmètre du pilotage de la production informatique

Le Pôle Système d'Information déploie des moyens technologiques permettant de satisfaire les exigences de sécurité des métiers et en garantit le bon fonctionnement dans le respect :

- ✓ Des bonnes pratiques en vigueur ;
- ✓ Des principes émanant des Directives de Sécurité du Système d'Information ;

Sur le périmètre des systèmes d'information, la spécificité des missions assurées impose des responsabilités particulières inhérentes aux grandes natures d'activité couvertes :

- Des activités de production informatique permettant, par le recours à des technologies, infrastructures et processus opérationnels optimisés, de proposer aux métiers des systèmes d'information performants
- Des activités liées à des projets d'évolution des systèmes d'information de Covea Finance comprenant notamment :

• Des activités d'étude et de conseil auprès des métiers

• Des activités de gestion de projets pour le compte des métiers ou, plus globalement

• Des activités de conception/optimisation, réalisation, livraison et maintenance de solutions applicatives ou techniques

Ainsi, le Pôle Système d'Information doit :

- ✓ Décliner les directives de sécurité applicables dans les contextes techniques particuliers des infrastructures informatiques ;
- ✓ Concevoir, mettre en œuvre et administrer les services et mécanismes de sécurité nécessaires pour réduire et contrôler les vulnérabilités potentielles et fournir un environnement technique sécurisé ;
- ✓ Prendre en charge le traitement des incidents de sécurité affectant les ressources informatiques et télécoms ;
- ✓ Assurer un niveau standard de sécurité technique, sauf exigences particulières des métiers ;
- ✓ Veiller à la mise en place d'outils de mesures continues des risques techniques auxquels les infrastructures sont exposées (incidents, évolution des vulnérabilités…) et à l'exploitation des résultats ;
- ✓ Assurer un reporting trimestriel vers la Direction concernant les niveaux de risque intrinsèques aux environnements informatiques et de télécommunication.

2. Périmètre des projets d'évolution des systèmes d'informations

Tout projet d'évolution des systèmes d'information de Covea Finance mobilise une Maîtrise d'Ouvrage et une Maîtrise d'Œuvre chargée respectivement :

- ✓ D'exprimer les besoins fonctionnels liés au projet et de contrôler la conformité de la solution fournie à leur égard
- ✓ De construire la solution (notamment matérielle et logicielle) répondant aux besoins exprimés

Au titre de la sécurité :

- ✓ La Maîtrise d'Ouvrage projet :

• Exprime les besoins de sécurité SI du projet (disponibilité (D), intégrité (I), confidentialité (C), preuve (P)) et rédige le cahier des charges correspondant ;

• Mène une analyse de risque détaillée dans les cas prévus par Covea Finance ;

• Valide au niveau ad hoc l'acceptation des risques résiduels ;

• S'assure de la mise en place effective des mesures de sécurité retenues.

- ✓ La Maîtrise d'Œuvre projet :

• Est responsable de la conformité de la solution retenue aux besoins DICP exprimés par la Maîtrise d'Ouvrage, tout en respectant les exigences de la PSSI et les directives de sécurité associées, notamment en matière de :

- O Conception, homologation et déploiement d'environnements informatiques (Serveurs, réseaux, postes de travail…) sécurisés ;
- O Conception d'architectures de sécurité réseau, systèmes et application ;
- O Développement sécurisé d'applications

• A en outre un devoir de conseil et de mise en garde auprès de la Maîtrise d'Ouvrage.

IV. Collaborateurs

Toute personne autorisée à accéder aux systèmes d'information de Covea Finance agit dans le cadre strict des missions qui lui sont confiées et doit appliquer les principes comportementaux issus de la Charte ainsi que les règles de sécurité édictées dans le cadre de ses activités et/ou des projets auxquels elle est amenée à participer. Elle doit ainsi :

- ✓ Respecter les obligations légales et réglementaires ;
- ✓ Respecter les procédures et règles de sécurité ;
- ✓ Contribuer par son comportement à la protection du patrimoine informationnel de Covea Finance contre toute menace d'origine malveillante (piratage, fraude, sabotage, renseignement) ou accidentelle (incidents, erreurs) et tout risque afférent (intrusion, divulgation, altération, destruction…) susceptibles de porter atteinte aux intérêts de Covea Finance ;
- ✓ Participer à toute action de sensibilisation à la sécurité initiée par sa hiérarchie ou par Covea Finance ;
- ✓ Informer sa hiérarchie ou le responsable du Pôle SI de tout incident, anomalie ou infraction à la politique de sécurité ou à ses règles d'application.

V. Partenaires et prestataires

Les partenaires et prestataires qui sont amenés à intervenir au sein de Covea Finance ou à accéder à ses systèmes d'information doivent être invités à se comporter comme des

personnels de Covea Finance. Lorsque cela s'avère nécessaire, certaines catégories de partenaires ou de prestataires devront s'engager contractuellement à respecter les règles de sécurité en vigueur. La pertinence des engagements demandés devra être régulièrement remise en cause par Covea Finance.

Les accords contractuels avec des prestataires informatique en nuage (cloud) contiendrons une clause d'audit. Une appréciation des risques sera réalisée en amont de la contractualisation selon la méthodologie EBIOS Risk Manager.

VI. Contrôle interne

Le contrôle interne s'assure du respect du cadre législatif et réglementaire auquel est soumis Covéa Finance, de l'efficacité et l'efficience de ses opérations et de la disponibilité des informations financières et non financières, ainsi que leur fiabilité.

VII. Audit

L'audit permet d'analyser la qualité des dispositifs de contrôles internes et de s'assurer que les principaux risques auxquels Covéa Finance peut être confrontée sont efficacement gérés. Le service d'audit interne agit à la demande de la direction générale

5. Gestion de la PSSI

I. Validité de la PSSI

La PSSI est diffusée via l'intranet de Covea Finance et s'applique à compter de sa publication.

II. Évolution de la PSSI

La PSSI est révisée au moins tous les ans et à l'occasion de chaque changement significatif affectant Covea Finance, par exemple :

- ✓ Modification de sa stratégie avec impact sur ses objectifs de sécurité ;
- ✓ Evolution de son organisation ou de ses activités ;
- ✓ Evolution du contexte législatif ou réglementaire ;
- ✓ Apparition de nouvelles menaces ;
- ✓ Evolutions requises à l'issue des processus de contrôle interne et des audits interne mis en œuvre ;
- ✓ Evolutions de l'architecture des systèmes d'informations et de ses interconnexions ;

Toute évolution de la PSSI est placée sous la responsabilité du Responsable de la Sécurité des Systèmes d'informations (RSSI) et est **soumise à la validation du CoDir.**

III. Contrôle de l'application de la PSSI

La démarche de contrôle de l'application de la PSSI (et de ses directives thématiques) s'inscrit dans le respect des bonnes pratiques professionnelles et des obligations réglementaires. Celle-ci mobilise différents acteurs internes ou externes selon l'objet des contrôles, dans le respect des principes de séparation des pouvoirs :

- ✓ **Contrôles de niveau 1 :** Réalisés par les métiers, ils ont pour objet de s'assurer de manière permanente de la maîtrise des risques de sécurité SI pesant sur les processus / activités de Covea Finance, dans le respect des procédures définies. Les contrôles de premier niveau sont réalisés par le service Architecture et sécurité.

- ✓ **Contrôle de niveau 2** : Relevant du processus de contrôle interne, ils ont pour objet de s'assurer du respect du cadre législatif et réglementaire auquel est soumis Covéa Finance.

- ✓ **Contrôle de niveau 3** : Relevant du processus d'audit, ils ont pour objet d'analyser la qualité des dispositifs de contrôles internes et de s'assurer que les principaux risques auxquels Covéa Finance peut être confrontée sont efficacement gérés

6. Annexe

I. Composantes clés de la sécurité des systèmes d'informations

Conformément aux principes retenus par la norme ISO 27002 en la matière, la gestion des risques liés aux systèmes d'information recouvre les composantes suivantes :

COMPOSANTES	**OBJECTIFS**
Politique de sécurité de l'information	Définir les orientations générales en matière de gestion des risques liés aux systèmes d'information et obtenir l'engagement et le support indispensables du management.

Organisation de la sécurité de l'information	Définir les rôles et responsabilités des acteurs internes et externes en matière de cadrage & pilotage, déploiement, suivi et contrôle de la gestion des risques liés aux systèmes d'information de Covea Finance.
Sécurité des ressources humaines	Réduire les risques liés au facteur humain (erreurs, malveillance, fraude).
Gestion des actifs (Classification)	Inventorier et classifier les ressources des systèmes d'information afin de déployer une protection appropriée en fonction des enjeux qu'elles représentent à l'égard de l'activité.
Contrôle d'accès	Contrôler l'accès aux informations de Covea Finance en fonction des enjeux et exigences métiers.
Cryptographie	Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.
Infrastructure de gestion de clés ou PKI (Public Key Infrastructure)	Garantir l'efficacité et la sécurité des services de gestion des certificats à clés publiques.
Sécurité liée à l'exploitation	Assurer le maintien en conditions opérationnelles fiables et sécurisées de l'ensemble des ressources informatiques et télécommunications, support des processus manipulant de l'information au sein de Covea Finance.
Virtualisation des SI	Garantir la protection des applications hébergées sur des serveurs virtuels.
Réseau filaire, réseau WI-FI	Assurer la mise en place sécurisée et le maintien en condition de sécurité des réseaux d'accès au SI.
Sécurité des accès distants	Garantir la sécurité des accès au SI Covéa Finance à partir d'un réseau externe par du personnel Covéa Finance en situation de nomadisme ou par des tiers.
Acquisition, développement et maintenance des systèmes d'informations	S'assurer que la sécurité est prise en compte dans le cadre des nouveaux projets ou lors de leur évolution.

C2 - Interne

Bases de données	Assurer la sécurité des données stockées dans les bases de données.
Gestion des traces électroniques	Permettre de s'assurer que : o La collecte des informations n'est ni frauduleuse, ni déloyale, ni illicite o Les informations ne sont pas conservées au-delà de la durée prévue o Les informations ne sont pas communiquées à des personnes non autorisées o Les traitements font l'objet d'une sécurité optimale, afin qu'aucun détournement de finalité ne puisse avoir lieu.
Gestion des évènements de sécurité	Détecter « au fil de l'eau » des situations anormales, les analyser et, le cas échéant, engager dans les meilleurs délais les actions permettant d'y remédier.
Gestion des incidents liés à la sécurité de l'information	Enregistrer les incidents entraînant l'arrêt de l'activité. Protéger les processus critiques de Covea Finance de l'impact de sinistres des systèmes d'information. S'assurer de la remise en état rapide des systèmes après incidents.
Gestion d'une cyber-crise	Limiter l'impact d'une crise grâce à une organisation et une chaîne de commandement spécifique.
Aspects de sécurité de l'information dans la gestion de la continuité d'activité	Prendre en compte la sécurité de l'information dans la gestion de la continuité des activités de Covea Finance et garantir la disponibilité au quotidien des moyens de traitement de l'information
Sécurité opérationnelle	Mettre en place une équipe de sécurité proche des équipes opérationnelles permettant une réaction rapide face aux incidents de sécurité.
Conformité	Éviter tout manquement à des obligations légales, statutaires, réglementaires ou contractuelles du fait d'un dysfonctionnement impactant les systèmes d'informations.

C2 - Interne

Postes de travail	Protéger par des mesures adaptées : o Le poste de travail contre tout incident physique (détérioration, vol) ou logique (attaque virale) ; o Les données qu'il héberge et celles auxquelles il permet d'accéder (perte, destruction, altération, détournement, vol) ; o L'utilisateur, vis à vis d'opérations illicites, notamment au regard de la législation (usage de logiciels sans licence ou non autorisés).
Imprimantes multifonctions (IMF)	Garantir la sécurisation des imprimantes multifonctions par : o Le choix du fournisseur et la contractualisation ; o La sécurité physique des IMF ; o La configuration des IMF ; o La sécurité des flux et réseaux d'impression ; o Le contrôle des accès logiques.
Messagerie électronique	Assurer la sécurité de l'infrastructure qui supporte la messagerie électronique ainsi que les données qui y transitent.
Navigation Internet	La navigation Internet doit s'appuyer sur une architecture d'accès Internet fiable, des services sécurisés, des règles d'usage permettant de limiter les risques de compromission.
Protection contre les codes malveillants (virus, vers, chevaux de Troie, logiciel espions…)	Mettre en place des mesures de sécurité empêchant l'introduction de codes malveillants dans le SI, à défaut, les détecter et les bloquer.
Relation avec les fournisseurs	Garantir la protection des actifs informationnels accessibles aux fournisseurs. Maintenir les niveaux de service et de sécurité contractuellement convenus avec les prestataires.

C2 - Interne

Sécurité des services Cloud	Exiger du fournisseur, des services Cloud répondant aux règles de sécurité de Covéa Finance et réaliser des audits
Sécurité des sites Web	Garantir la sécurité des architectures et serveurs délivrant des services Web.
Téléphonie Mobile	Garantir l'usage sécurisé des téléphones mobiles gérés par Covéa Finance en contrôlant l'accès au téléphone, en assurant une gestion centralisée de la flotte via une plate-forme Mobile Device Management.
Téléphonie sur IP (ToIP)	Assurer la protection des communications sur IP.
Sécurité physique et environnementale	Se prémunir des dysfonctionnements ou sinistres résultant d'accès non autorisés aux sites du Groupe, ou d'événements environnementaux (incendie, dégâts des eaux, …).
Sensibilisation à la Sécurité SI	La sécurité des SI repose en très grande partie sur les comportements des personnes qui y ont accès. C'est pourquoi, leur sensibilisation aux bonnes pratiques comportementales à adopter pour les éviter constitue une action prioritaire de sécurité.

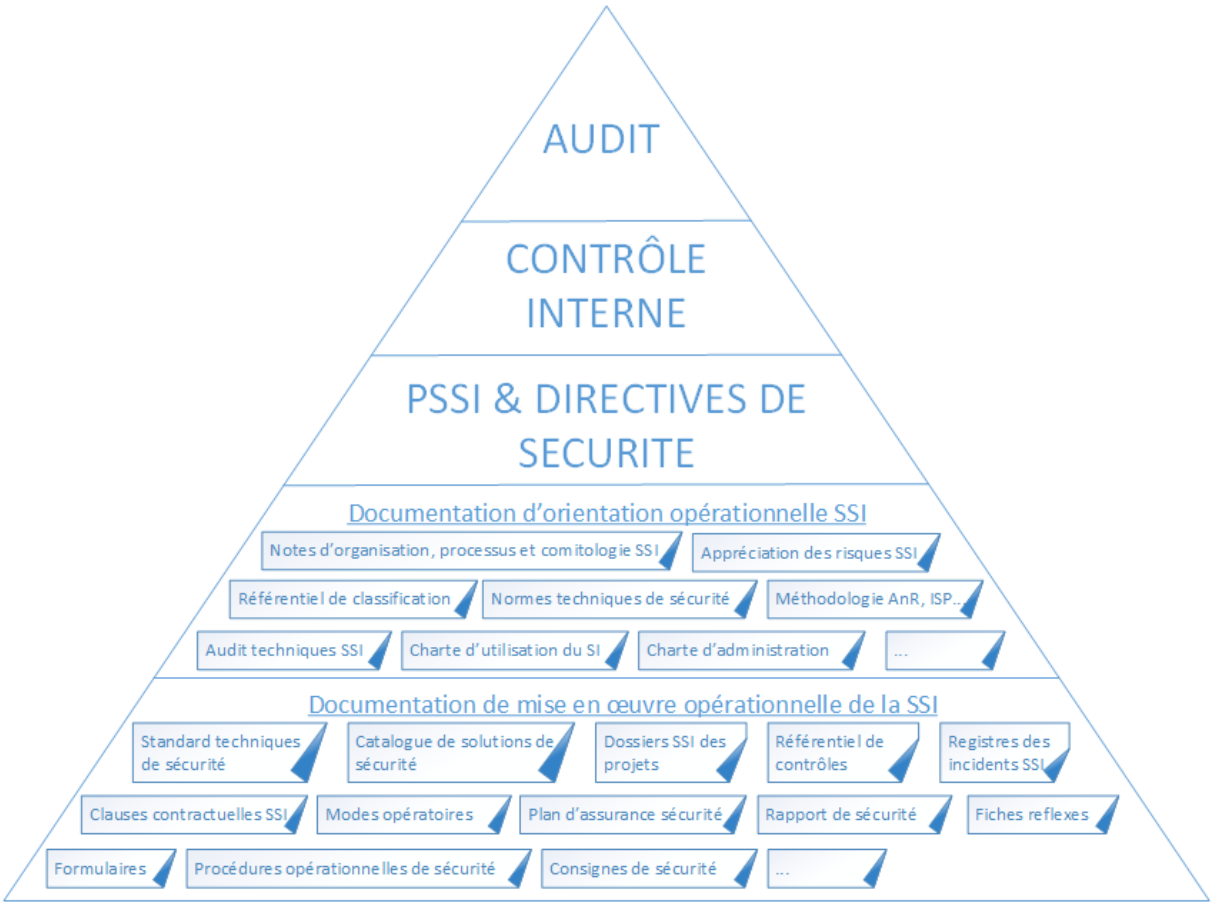
II. Articulation documentaire

C2 - Interne

Le schéma qui suit présente, dans les principes et sans être exhaustif, la manière dont la présente PSSI et ses directives de sécurité sont déclinées pour former l'ensemble du cadre documentaire de sécurité du SI de Covea Finance.

Ce schéma distingue :

- Le cadre l de sécurité SI (la présente PSSI et l'ensemble des directives de sécurité SI)
- Les documents d'orientation opérationnelle de sécurité SI, interfaces entre le cadre de sécurité SI et sa déclinaison documentaire opérationnelle
- Les documents de mise en œuvre opérationnelle de la sécurité SI qui traduisent au plus près des processus / activités les règles et principes issus du cadre de sécurité SI



III. Référentiel de directives

A date de la publication de la présente directive, la liste des directives de sécurité SI applicables est la suivante (avec mise en perspective vis-à-vis de la norme ISO 27002) :

Axe ISO 27002	**Directives**
Politique de sécurité de l'information	<cf. présente PSSI>
Organisation de la sécurité de l'information	<cf. présente PSSI + ensemble des directives>
Gestion des actifs	· Classification des informations
Contrôle d'accès	· Contrôle des accès logiques
Cryptographie	· Cryptographie · Infrastructure de gestion de clés
Sécurité physique et environnementale	· Sécurité physique et environnementale
Sécurité liée à l'exploitation	· Gestion et maintenance du SI · Protection contre les codes malveillants · Gestion des traces électroniques (*)
Sécurité des communications	· Sécurité des réseaux filaires · Sécurité des réseaux sans fils · Sécurité de la messagerie électronique · Sécurité de la téléphonie mobile (*) · Sécurité de la ToIP · Sécurité des accès distants (*) · Sécurité de la navigation sur internet (*)
Acquisition, développement et maintenance des systèmes d'information	· Intégration de la sécurité dans les projets · Sécurité des bases de données (*) · Sécurité des sites web (*)
Relation avec les fournisseurs	· Relation avec les fournisseurs · Sécurité des services Cloud (*)
Gestion des incidents liés à la sécurité de l'information	· Gestion des incidents de sécurité · Gestion d'une cyber-crise
Aspects de sécurité de l'information dans la gestion de la continuité d'activité	· Continuité de la sécurité SI

C2 - Interne

Conformité	· Conformité
Hors axes ISO 27002 (forte transversalité)	· Sécurité des postes de travail · Sécurité des imprimantes multifonctions (IMF) · Sécurité des systèmes d'exploitation · Sécurité de la virtualisation des S.I.

(*) : « Positionnement principal » fourni à titre indicatif dans la mesure où certaines directives peuvent adresser plusieurs des axes de l'ISO 27002.

C2 - Interne