Référence	Nom	Date de MAJ
4.14	**DÉTECTION, PRÉVENTION ET GESTION DES RISQUES DE CYBERSÉCURITÉ**	03 Novembre 2021 13 mars 2023 20 février 2025

1. Contexte et environnement réglementaire

La présente procédure a pour objectif de décrire le dispositif mis en place par la société de gestion pour détecter, prévenir et gérer le risque de cybersécurité d'Elevation Capital Partners.

Les procédures mises en œuvre par la société de gestion relatives au plan de continuité d'activité, à l'enregistrement et la conservation des données ainsi que la charte informatique participent également au dispositif global de prévention, de détection et de gestion des risques de cybersécurité.

Recueil	Article	Thématique abordée
RG AMF	Articles 318-1, 4, 6, 58 à 61	Règles d'organisation Dispositif de conformité Responsabilité des dirigeants Gestion des risques Externalisation Enregistrement et conservation des données
Règlement délégué (UE) n° 231/2013	Articles 13, 22, 38 à 41, 57, 60 à 62	
Règlement délégué (UE) n°2017/565	Articles 21 à 25	
Guide professionnel AFG relatif à la cybersécurité	Tous	Bonnes pratiques concernant la cybersécurité
Synthèses des contrôles SPOT sur le dispositif de cybersécurité des sociétés de gestion de portefeuille	Tous	Bonnes et mauvaises pratiques concernant le dispositif de cybersécurité relevées par l'AMF lors de ses contrôles SPOT
Loi sur la sécurité informatique et libertés n°78-17 du 06/01/1978	Tous	-
Règlement européen 2022/2554	Tous	Règlement DORA entré en vigueur le 17/01/2025

2. Présentation du risque de cybersécurité

Le risque de cybersécurité découle de toute atteinte malveillante potentielle, interne ou externe, à l'une des caractéristiques clés du système d'information d'une société de gestion de portefeuille, c'est-à-dire sa disponibilité, son intégrité, la confidentialité des données qu'il traite et la traçabilité des actions.
Ce risque peut cibler les placements collectifs et/ou les mandats gérés : il s'assimile alors à un risque opérationnel mais ne s'y réduit pas. Sa réalisation peut en effet également conduire à une non-conformité réglementaire de la société de gestion dans les domaines relatifs à l'existence et au maintien :

- ✓ Du niveau de fonds propres réglementaires (ces derniers pouvant être obérés en cas de rupture d'activité) ;
- ✓ D'une politique rigoureuse de conservation et de maintien des données opérationnelles, notamment aux fins de contrôles par l'AMF (sur les transactions opérées et la lutte anti-blanchiment par exemple) ;
- ✓ D'un plan de continuité d'activité (PCA) adapté, testé et efficace (une attaque cyber pouvant rendre inutilisables les infrastructures informatiques de la société de gestion et/ou les installations de secours et/ou les sauvegardes effectuées) ;
- ✓ De moyens (informatiques) adaptés et suffisants ;
- ✓ D'un dispositif solide de protection des données sensibles (relatives aux investisseurs, aux fonds et aux mandats) et de respect du règlement européen général sur la protection des données (RGPD).

3. Les différentes typologies d'attaques cybers

Les attaques malveillantes potentielles peuvent prendre plusieurs formes. Les méthodes les plus utilisées sont les suivantes :

A) Le rançongiciel ou le ransomware

Cette méthode consiste à accéder aux données de l'entreprise afin de les pirater et d'exiger une rançon.

B) L'hameçonnage ou le phishing

Il consiste à envoyer des mails frauduleux auprès des employés afin de compromettre des informations personnelles telles que des identifiants et mots de passe.

C) Botnets

Il s'agit d'un réseau d'ordinateurs privés infectés par des logiciels malveillants et contrôlés comme un groupe à l'insu de leurs propriétaires.

Un manipulateur de botnet peut prendre le contrôle d'un ordinateur via différentes manières tels les téléchargements drive by (logiciel qui s'installe automatiquement suite à la consultation d'un mail ou d'un site piégé) ou les courriers électroniques. Dans les deux cas, l'objectif reste le même : envoyer du code pirate sur l'ordinateur de l'utilisateur et en prendre le contrôle.

D) Le cryptominage

Dans le cadre de cette méthode, les pirates demandent à la victime de cliquer sur un lien malveillant dans un courrier électronique qui charge le code de cryptographie sur l'ordinateur, ou alors ils infectent un site Web ou une annonce en ligne avec du code JavaScript qui s'exécute automatiquement une fois chargé dans le navigateur de la victime.

4. Les conséquences d'une attaque cyber

La cybersécurité est d'une importante capitale pour la société de gestion. En effet, en cas d'une attaque cyber, les conséquences potentielles pour la société de gestion peuvent être :

- ✓ Opérationnelles ;
- ✓ Financières ;
- ✓ Juridiques ;
- ✓ Réputationnelles ; et
- ✓ Réglementaires.

5. Dispositif mis en place par la société de gestion

Afin de prévenir, détecter et gérer les risques de cybersécurité, la société de gestion a mis en place un dispositif spécifique.

A) Gouvernance de la cybersécurité

Afin d'assurer une gouvernance efficace du risque de cybersécurité, ce dernier fait l'objet d'un point formalisé a minima deux fois par an dans le cadre du comité des risques auquel participe le responsable des risques, également RCCI, ainsi que les membres de la Direction. Le comité pourra également se réunir exceptionnellement en cas par exemple de survenance d'un risque cyber.

Ce comité est habilité à prendre toute décision relative à la gestion du risque de cybersécurité.

B) Cartographie des risques de cybersécurité

La société de gestion a mis en place une cartographie des risques de cybersécurité.

Elle permet notamment d' :

- ✓ Identifier l'ensemble des risques de cybersécurité de la société de gestion ;
- ✓ Evaluer le risque brut de chacun d'entre eux pour la société de gestion ;
- ✓ Indiquer les mesures mises en place afin de prévenir et éviter ces risques ;
- ✓ Evaluer le risque net de chaque risque identifié après avoir pris en compte les mesures préventives mises en place par la société de gestion.

Cette cartographie est mise à jour régulièrement et a minima annuellement.

C) Mesures de prévention et sensibilisation des collaborateurs

Des mesures sont mises en place par la société de gestion afin de prévenir le risque de cybersécurité, notamment :

- ✓ La ségrégation du réseau informatique ;
- ✓ La sauvegarde régulière des données sur un réseau indépendant ;
- ✓ La sécurisation des locaux ;
- ✓ La vigilance constante des collaborateurs ;
- ✓ La signature par chaque collaborateur d'une charte informatique ;
- ✓ La gestion des habilitations ; ou encore
- ✓ La double authentification pour accéder au réseau à distance.

L'ensemble des mesures de prévention sont identifiées et présentées dans la cartographie des risques de cybersécurité.

Par ailleurs, les collaborateurs sont sensibilisés aux risques de cybersécurité, aux bonnes pratiques à adopter ainsi qu'aux dispositifs mis en place par la société de gestion. Cette sensibilisation s'effectue par le biais d'un support de formation mis en place par le RCCI et remis aux collaborateurs dans le cadre de leur embauche..

Par ailleurs, le groupe Inter Invest a mis en place, à l'aide de son prestataire informatique Itaia un portail de sensibilisation aux risques de cybersécurité. Un premier questionnaire d'évaluation est envoyé systématiquement à tous les nouveaux collaborateurs afin d'évaluer leur niveau. Celui-ci permet de prioriser et adapter certains cours en fonction des sujets les moins maitrisés par le nouvel entrant.
Les collaborateurs doivent avoir atteint un taux de réussite de 80% afin de valider chaque formation mensuelle obligatoire.
Le portail permet au collaborateur, mais aussi à la Direction, de connaître les statistiques relatives à la formation et notamment :

- ✓ Le nombre de module pour le collaborateur ;
- ✓ Le nombre de cours débuté ;
- ✓ Le nombre de cours finalisé ; ainsi que
- ✓ La note moyenne obtenue.

Un test de phising est également mis en place tous les mois. Si lors des tests de phishing, des collaborateurs ont été identifiés comme plus sensibles au risque de cybersécurité, une formation complémentaire sera dispensée à ces derniers.
L'outil en ligne d'Itaia permet aux collaborateurs et à la société de gestion de connaître les statistiques relatives au nombre de mails ouverts, au nombre de liens suivis, au nombre de données compromises et au nombre de tentatives identifiées par les collaborateurs.

D) Contrôle et test

Afin de pouvoir s'assurer de la conformité du dispositif relatif à la cybersécurité et de pouvoir évaluer la sensibilité des collaborateurs aux risques de cybersécurité, différents contrôles et test sont réalisés par la société de gestion ou tout prestataire habilité :

Teneur du contrôle ou du test	Réalisé par	Périodicité
Un test d'intrusion sur le système d'information de la société de gestion est réalisé afin de mesurer la robustesse du dispositif de cybersécurité en place et de vérifier l'efficacité de prise en compte des vulnérabilités identifiées lors du test antérieur	Remplacé chaque année pour éviter les habitudes	Annuel
Un faux mail frauduleux simulant une tentative de phishing est envoyé à l'ensemble des collaborateurs afin de pouvoir déterminer leur niveau de sensibilité au risque cyber sécurité	Itaia	Mensuel

E) Charte informatique

Une charte informatique a été mise en place par le Groupe Inter Invest. Elle édicte les règles et les bonnes pratiques que se doivent de respecter les collaborateurs dans le cadre de l'utilisation des systèmes d'information de la société de gestion. Certaines de ses dispositions permettent notamment de prévenir les risques de cybersécurité.

L'ensemble des collaborateurs doivent signer cette charte et s'engagent à respecter les règles et bonnes pratiques qui y sont exposées.

6. La réaction en cas d'attaque

En cas d'attaque, la société de gestion devra formaliser son analyse et le plan d'action qu'elle met en œuvre. Les différentes étapes sont :

- ✓ Cerner l'attaque et définir s'il s'agit d'une crise (toute l'activité) ou d'un accident (isolé pour un utilisateur) ;
- ✓ Comprendre l'attaque et définir une stratégie de réponse ;
- ✓ Convoquer la cellule de crise et son organe de communication (cf. *procédure 4.06 relative au plan de continuité d'activité*) ;
- ✓ Déterminer les dommages potentiels pour l'entreprise ;
- ✓ Déterminer la durée de l'attaque ;
- ✓ Documenter tout le processus de l'attaque pendant l'attaque ;
- ✓ Suivre la résolution de l'attaque.

Cette analyse sera formalisée dans le cadre du comité des risques qui se réunira en cas de survenance d'un tel événement.

Si besoin, la société de gestion devra étudier la possibilité d'activer le PCA et mettre en place un plan de contre-attaque et de récupération des données. Par ailleurs selon les impacts, les clients et/ou le régulateur devront en être informés.

Dans tous les cas, l'incident devra être renseigné dans le registre des incidents (cf. *procédure 4.03 Procédure alertes et dysfonctionnements*)

7. Digital Operational Resilience Act (DORA)

Le règlement DORA (Digital Operational Resilience Act), définit un cadre détaillé et complet sur la résilience opérationnelle numérique pour les entités financières, et s'applique donc aux sociétés de gestion (SGP).

Le texte est entré en vigueur le 17 janvier 2025 et impose des obligations aux entités financières, mais également à leurs prestataires de services numériques.

Ceux-ci devront revoir régulièrement leurs procédures, contrats, mécanismes et outils assurant la sécurité des systèmes d'information.

Les dispositions relatives à la contractualisation avec les TIC sont prévues dans la procédure de sélection et de suivi des prestataires (référence 4.04).

ECP s'intègre dans une démarche groupe avec Inter Invest concernant sa stratégie de résilience numérique puisque les outils informatiques utilisés par la société de gestion sont mis à disposition par Inter Invest et la maintenance informatique sous délégué au prestataire Itaia.

Les attendus liés à DORA sont par ailleurs repris en annexe 1 de la présente procédure.

Conformément à l'article 4 du règlement, un principe de proportionnalité s'applique. Les dispositions à mettre en œuvre au titre du règlement DORA doivent en effet tenir compte de la taille et du profil de risque global ainsi que de la nature, de l'ampleur et de la complexité des services, activités et opérations de la société de gestion.

ECP s'attèlera en 2025, conjointement avec le Groupe Inter Invest, à la déclinaison des attendus règlementaires liés au règlement DORA.

8. Dispositif de contrôle

Selon la périodicité définie dans le plan de contrôle, le RCCI mène à bien l'analyse de la conformité du dispositif de cybersécurité ainsi que le respect des dispositions définies dans la procédure. Le RCCI s'assure également de mener une veille réglementaire sur ce sujet.

La fonction de contrôle périodique s'assure en 3ème niveau du respect des obligations règlementaires applicables.

Signatures de la Direction et du RCCI :

Benoit Petit Certified by yousign	Julien Hugot Certified by yousign	Benjamin Cohen Certified by yousign	Laurent Casanova Certified by yousign

Annexe 1 : Stratégie de résilience numérique et livrables attendus dans DORA

Cartographie des livrables attendus dans DORA :