



Politique de gestion des risques

Responsable de la politique : Responsable recherche et développement

Date d'entrée en vigueur : 04 Mars 2024

Nom de l'entreprise :	Evalandgo Software	
Responsables de la politique :	Valentin Boschatel	Téléphone :
Date d'entrée en vigueur :	04 Mars 2024	Date de révision : 10 Mars 2025
Dernier avis :	10 Mars 2025	Prochaine révision : 16 Mars 2026

Visée :

Définir des actions pour faire face aux risques et aux potentialités en matière de sécurité de l'information de Evalandgo Software. Définir un plan pour atteindre les objectifs en matière de sécurité de l'information et de protection de la vie privée.

Champ d'application :

- Tous les systèmes informatiques de Evalandgo Software qui traitent, stockent ou transmettent des données confidentielles, privées ou critiques.
- Les risques susceptibles d'affecter les objectifs à moyen et long terme de Evalandgo Software doivent être pris en compte, de même que les risques rencontrés dans la prestation quotidienne des services.
- Les systèmes et processus de gestion des risques de Evalandgo Software seront ciblés de manière à en tirer le maximum d'avantages sans alourdir la charge bureaucratique et sans affecter, en fin de compte, la prestation de services de base à l'entreprise.
- Evalandgo Software tiendra donc compte de l'importance relative du risque lors du développement de systèmes et du processus de gestion des risques.
- La présente politique s'applique à tous les employés de Evalandgo Software et à toutes les parties externes, y compris, mais sans s'y limiter, les consultants et sous-traitants de Evalandgo Software, les partenaires commerciaux, les fournisseurs, les prestataires de services externalisés et autres entités tierces ayant accès aux réseaux et aux ressources du système de Evalandgo Software.

Déclaration de gestion des risques

Une gestion inadéquate des risques informatiques expose Evalandgo Software à des risques tels que la compromission des systèmes, services et informations du réseau de Evalandgo Software ou de ses clients, des cyberattaques, des problèmes contractuels ou juridiques. Evalandgo Software s'assurera que la gestion des risques joue un rôle essentiel dans la gouvernance et la gestion de l'entreprise aux plans stratégique et opérationnel. L'objectif d'une politique de gestion des risques est de s'assurer que l'entreprise atteint les objectifs opérationnels qu'elle s'est fixés.

Stratégie de gestion des risques

Evalandgo Software a développé des processus pour identifier les risques susceptibles d'entraver la réalisation de ses objectifs stratégiques et opérationnels. Evalandgo Software s'assurera donc qu'elle a mis en place les moyens d'identifier, d'analyser, de contrôler et de surveiller les risques

stratégiques et opérationnels auxquels elle fait face à l'aide de la présente politique de gestion des risques, laquelle se fonde sur les meilleures pratiques.

Evalandgo Software veillera à ce que la stratégie et la politique de gestion des risques soient régulièrement réexaminées et à ce que les fonctions d'audit interne soient chargées de garantir les points suivants :

- La politique de gestion des risques est appliquée aux domaines pertinents au sein de Evalandgo Software ;
- La politique de gestion des risques et son application opérationnelle font l'objet d'une révision régulière ;
- La non-conformité est signalée à des responsables appropriés de l'entreprise ainsi qu'aux autorités concernées.

Application pratique de la gestion des risques

Evalandgo Software a adopté un format normalisé à utiliser pour l'identification des risques, leur classification et leur évaluation.

Le format est basé sur les normes et cadres NIST et ISO suivants :

- Norme ISO 27005
- NIST 800-30
- NIST 800-37

Les risques sont évalués et classés en fonction de leur impact et de leur probabilité d'occurrence. Une évaluation formelle des risques et des tests d'intrusion du réseau seront effectués au moins une fois par an et prendront en compte les résultats de toute activité de gestion des vulnérabilités techniques réalisée conformément à la politique de sécurité des activités.

Catégories de risques

Evalandgo Software examinera et évaluera les risques dans l'ensemble de l'entreprise. Les catégories de risques à prendre en compte pour l'évaluation sont les suivantes :

- Risque de réputation ;
- Risque contractuel ;
- Risque lié à la réglementation ou la conformité ;
- Risque économique ou financier ;
- Risque de fraude.
- Vie privée ;
- Environnement et durabilité ;
- Impact sur les personnes ;
- Utilisation des services cloud
- Capacité opérationnelle.

Chaque risque sera évalué en fonction de sa probabilité et de son impact. Cette évaluation sera effectuée sur une échelle de 1 à 5. L'impact peut aller de 1 (« Très faible impact ») à 5 (« Très fort impact ») et la probabilité peut aller de 1 (« Très peu probable ») à 5 (« Très probable »).

Critères de risques

Les critères permettant de déterminer le niveau de risque correspondant à la probabilité associée à l'impact d'un événement ayant un effet négatif sur la confidentialité, la disponibilité ou la confidentialité des informations de l'organisation et des clients, de données à caractère personnel ou des systèmes d'information de l'entreprise.

Pour toutes les mentions de risques indiquées dans des documents tels que les évaluations des risques, les analyses de vulnérabilité, les tests d'intrusion, les programmes de prime aux bugs, etc., la direction de Evalandgo Software se réserve le droit de modifier les classements de risques en fonction de son évaluation de la nature et du caractère critique du traitement du système, ainsi que de la nature, du caractère critique et du caractère exploitable (ou d'autres facteurs et considérations pertinents) de la vulnérabilité identifiée.

Réponse aux risques, traitement et suivi

Les risques seront classés par ordre de priorité et conservés dans un registre des risques où ils seront classés par ordre de priorité et cartographiés en utilisant l'approche contenue dans la présente politique. Les réponses suivantes au risque devront être utilisées :

- **Atténuer** : Evalandgo Software peut prendre des mesures ou utiliser des stratégies pour réduire les risques.
- **Accepter** : Evalandgo Software peut décider d'accepter et de surveiller le risque pour le moment. Cela peut être nécessaire pour certains risques découlant d'événements externes.
- **Transférer** : Evalandgo Software peut décider de transmettre le risque à une autre partie. Par exemple, il peut être possible de conclure des conditions contractuelles pour s'assurer que le risque n'est pas supporté par Evalandgo Software ; contracter une assurance peut aussi être approprié pour se protéger contre les pertes financières.
- **Éviter** : le risque peut être tel que Evalandgo Software peut décider de cesser l'activité ou de la modifier de manière à mettre fin au risque.

Lorsque Evalandgo Software choisit une réponse à un risque autre que « Accepter » ou « Éviter », elle doit élaborer un plan de traitement du risque.

Procédures de gestion des risques

La procédure de gestion des risques répondra aux critères suivants :

1. Evalandgo Software tiendra un registre et un plan de traitement des risques.
2. Les risques sont classés selon leur « probabilité » et leur « gravité/impact » comme critique, élevé, moyen, faible ou négligeable.
3. Le risque global est déterminé en combinant la probabilité et l'impact.
4. Lorsque cela est possible, les risques peuvent être évalués pour estimer les pertes monétaires potentielles.
5. Evalandgo Software répondra aux risques de manière prioritaire. Cette priorité accordée à la correction des problèmes tiendra compte de la probabilité et de l'impact des risques, des coûts, des efforts de travail à fournir et de la disponibilité des ressources. Plusieurs actions correctives peuvent être prises simultanément.
6. Des rapports réguliers seront présentés aux membres de la direction de Evalandgo Software pour s'assurer que les risques sont limités de manière appropriée et conformément aux priorités et objectifs opérationnels.

Sécurité de l'information dans la gestion de projet

Evalandgo Software considère que le risque de sécurité des informations fait partie du cadre de tous les projets de nature technique ou pouvant présenter un risque pour l'entreprise, quelle que soit leur taille, leur durée ou leur domaine. De la planification initiale à la fin d'un projet, l'évaluation des risques de sécurité de l'information et leur atténuation est vitale, notamment grâce à :

- des évaluations initiales des risques en matière de sécurité de l'information,
- l'identification en amont et le traitement des exigences de sécurité de l'information, et
- l'évaluation et la gestion continues des risques, notamment en ce qui concerne la communication interne et externe du projet.

Rôles et responsabilités

Le tableau suivant présente les activités et responsabilités spécifiques en matière de gestion des risques associées à chaque rôle.

Rôle	Responsabilité
Président/PDG	Responsable en dernier ressort de l'acceptation et/ou du traitement de tout risque pour l'entreprise.
Directeur de l'information	Peut approuver l'évitement, la correction, le transfert ou l'acceptation de tout risque mentionné dans le registre des risques.
Responsable informatique / Ingénieur système	Doit être responsable de l'identification et de l'élaboration du plan de traitement de tous les risques liés à la sécurité de l'information. Cette personne est chargée de communiquer les risques aux membres de la direction et d'adopter les traitements des risques conformément aux directives de la direction.

Autres ressources

04- Politique d'évaluation et de traitement des risques de l'ISMS

Pour consulter le registre des risques actuel, voir <https://app.vanta.com/risk-management/risk-register>

Champ d'application de la norme ISO 27001/27701

ISO 27001 6.1 et 6.2

Version	Date	Description	Auteur	Approuvé par
1.0	03-Mar-2024	Mise en œuvre initiale	Hugo Bachelet	Valentin Boschattel
1.1	10-Mar-2025		Hugo Bachelet	Valentin Boschattel

ANNEXE A - Processus d'évaluation des risques

Vous trouverez ci-dessous une vue d'ensemble du processus utilisé par Evalandgo Software pour évaluer et gérer les risques liés à la sécurité de l'information.

Le processus décrit ci-dessous est basé sur la norme NIST 800-30 et fournit des directives à Evalandgo Software sur la manière de procéder pour :

- Préparer et mener une évaluation efficace des risques ;
- Communiquer et partager les résultats de l'évaluation et les informations liées aux risques ;
- Gérer et maintenir les risques sur une base continue.

Le processus d'évaluation des risques comprend les étapes suivantes :

1. Préparer l'évaluation
2. Mener l'évaluation
3. Communiquer l'évaluation
4. Gérer l'évaluation

Étape 1 : Préparer l'évaluation

L'objectif de cette étape est d'établir le contexte de l'évaluation des risques. Pour ce faire, procédez comme suit :

- Déterminez le but de l'évaluation
 - Déterminez les informations que l'évaluation doit fournir et les décisions qu'elle doit appuyer.
- Identifiez la portée de l'évaluation
 - Déterminez la fonction ou le processus organisationnel applicable, le délai associé et toute considération architecturale ou technologique applicable.
- Identifiez les hypothèses ou les contraintes associées à l'évaluation
 - Déterminez les hypothèses dans les domaines clés pertinents pour l'évaluation des risques, notamment :
 - Priorités organisationnelles ;
 - Objectifs commerciaux ;
 - Disponibilité des ressources ;
 - Compétences et expertise de l'équipe d'évaluation des risques.
- Identifiez les sources d'information
 - Schémas architecturaux/technologiques et configurations de systèmes ;
 - Exigences légales et réglementaires ;
 - Sources de menaces ;
 - Événements de menace ;
 - Vulnérabilités et conditions d'influence ;
 - Impacts potentiels ;
 - Contrôles existants.

Étape 2 : Mener l'évaluation

L'objectif de cette étape est de dresser une liste des risques liés à la sécurité de l'information qui peuvent être classés par ordre de priorité en fonction du niveau de risque et utilisés pour éclairer les décisions en matière de réponse aux risques. Pour ce faire, procédez comme suit :

- Identifiez les sources de menaces
 - Déterminez et caractérisez les sources de menaces pertinentes et préoccupantes pour Evalandgo Software, y compris, mais sans s'y limiter :
 - Humain (Intentionnel ou Non intentionnel / Interne ou Externe) ;
 - Environnement ;
 - Facteurs naturels
 - Système ou équipement ;
 - Tenez compte des éléments suivants lors de l'identification des sources de menace :
 - Capacités
 - Motif / Intention ;
 - Personnes, processus et/ou technologies intentionnellement ciblés ;
 - Personnes, processus et/ou technologies ciblés de manière non intentionnelle.
- Identifiez les événements menaçants
 - Déterminez quels événements de menace pourraient être produits par les sources de menaces identifiées et susceptibles d'avoir un impact sur Evalandgo Software.
 - Examinez la pertinence des événements et les sources qui pourraient être à l'origine de ces événements.
- Identifiez les vulnérabilités
 - Déterminez les vulnérabilités associées aux personnes, aux processus et/ou aux technologies susceptibles d'être exploitées par les sources de menaces et les événements représentant une menace, qui ont été identifiés.
 - Tenez compte de toutes les conditions susceptibles d'influer sur la réussite de l'exploitation et d'y contribuer.

- Déterminez la probabilité
 - Déterminez la probabilité que les sources de menace identifiées soient à l'origine des événements identifiés représentant une menace et qu'elles parviennent à exploiter les vulnérabilités identifiées.
 - Tenez compte des éléments suivants pour déterminer la probabilité :
 - Caractéristiques des sources de menace susceptibles de déclencher les événements.
 - Capacités
 - Motif/Intention ;
 - Opportunité.
 - Les vulnérabilités et/ou les conditions d'influence identifiées
 - L'exposition de Evalandgo Software en fonction des mesures de sauvegarde/contre-mesures prévues ou mises en œuvre pour empêcher ou atténuer de tels événements.
- Déterminez l'impact
 - Déterminez l'impact sur les objectifs commerciaux, les activités, les actifs, les individus, les clients et/ou les autres structures de Evalandgo Software en tenant compte des éléments suivants :
 - Impacts commerciaux/opérationnels ;
 - Dommages financiers ;
 - Atteinte à la réputation ;
 - Questions juridiques ou réglementaires.
 - Lors de la définition de l'impact, prenez également en considération toute mesure de sauvegarde/contre-mesure planifiée ou mise en œuvre par Evalandgo Software qui permettrait d'atténuer ou de réduire l'impact.
- Déterminez le risque
 - Déterminez les risques globaux liés à la sécurité de l'information pour Evalandgo Software en combinant les éléments suivants :
 - La probabilité que l'événement se produise.
 - L'impact qui découlerait de l'événement.
 - Le risque pour Evalandgo Software est proportionnel à la probabilité et à l'impact d'un événement.
 - Événement de risque plus élevé : est plus susceptible de se produire et l'impact qui en résulte sera plus important.
 - Événement à bas risque : est moins susceptible de se produire et l'impact qui en résultera sera peu important voire inexistant.

Étape 3 : communiquer et partager les résultats de l'évaluation des risques

L'objectif de cette étape est de veiller à ce que les décideurs de Evalandgo Software et la direction disposent des informations appropriées sur les risques afin d'éclairer et d'orienter les décisions en la matière.

- Communiquez les résultats
 - Communiquez les résultats de l'évaluation des risques aux décideurs et aux dirigeants de Evalandgo Software afin de les aider à prendre des décisions fondées sur les risques et d'obtenir le soutien nécessaire pour la réponse aux risques.
 - Partagez l'évaluation des risques et les renseignements connexes avec le personnel approprié de Evalandgo Software afin de soutenir les efforts de réponse aux risques.

Étape 4 : gérer l'évaluation

L'objectif de cette étape est de tenir à jour les connaissances spécifiques relatives aux risques encourus par Evalandgo Software. Les résultats des évaluations éclairent et orientent les décisions fondées sur les risques et guident les efforts continus de réponse aux risques.

- Surveillez les facteurs de risque
 - Effectuez un suivi permanent des facteurs de risque qui contribuent à l'évolution des risques pour les objectifs commerciaux, les activités, les actifs, les individus, les clients et/ou les autres structures de Evalandgo Software.
- Gérez et mettez à jour l'évaluation
 - Mettez à jour les évaluations des risques existantes en utilisant les résultats du suivi permanent des facteurs de risque et en procédant à des évaluations supplémentaires, au moins une fois par an.

ANNEXE B - Matrice d'évaluation des risques et clé de description

<i>RISQUE= PROBABILITÉ X IMPACT</i>	PROBABILITÉ				
IMPACT	Très peu probable : 1	Peu probable : 2	Assez probable : 3	Probable : 4	Très probable : 5
Très fort impact : 5	5	10	15	20	25
Fort impact : 4	4	8	12	16	20
Impact moyen : 3	3	6	9	12	15
Faible impact : 2	2	4	6	8	10
Très faible impact : 1	1	2	3	4	5

NIVEAU DE RISQUE	DESCRIPTION DU RISQUE
Faible (1 à 4)	Un événement représentant une menace peut avoir un effet négatif limité sur les opérations de l'entreprise, ses capacités à remplir sa mission, les actifs, les individus, les clients ou d'autres entreprises.
Moyen (5 à 12)	Un événement représentant une menace peut avoir un effet négatif significatif sur les opérations de l'entreprise, ses capacités à remplir sa mission, les actifs, les individus, les clients ou d'autres entreprises.
Élevé (15 à 25)	Un événement représentant une menace peut avoir un effet négatif grave sur les opérations de l'entreprise, ses capacités à remplir sa mission, les actifs, les individus, les clients ou d'autres entreprises.

NIVEAU DE PROBABILITÉ	DESCRIPTION DE LA PROBABILITÉ	NOTE (NUMÉRIQUE)
Très peu probable (1)	Une menace est si peu probable que l'on peut supposer qu'elle ne se produira pas. Une source de menace n'a pas la motivation ou les capacités de passer à l'action, ou des contrôles ont été mis en place pour empêcher ou entraver de manière significative l'exploitation de la vulnérabilité.	1
Peu probable (2)	Une menace est peu probable, mais il existe une légère possibilité qu'elle se produise. Une source de menace n'a pas la motivation ou les capacités suffisantes pour passer à l'action, ou des contrôles ont été mis en place pour empêcher ou entraver l'exploitation de la vulnérabilité.	2
Assez probable (3)	Une menace est probable et l'on peut supposer qu'elle peut se produire. Une source de menace est motivée ou présente la capacité de passer à l'action, mais des contrôles pouvant réduire ou empêcher	3

	de manière significative l'exploitation réussie de la vulnérabilité ont été mis en place.	
Probable (4)	Une menace est probable et l'on peut supposer qu'elle se produira. Une source de menace est très motivée ou dispose de capacités et de ressources suffisantes pour passer à l'action, mais certains contrôles ont été mis en place et peuvent réduire ou empêcher l'exploitation réussie de la vulnérabilité.	4
Très probable (5)	Une menace est très probable et l'on peut supposer qu'elle se produira. Une source de menace est très motivée ou dispose des capacités ou des ressources suffisantes pour passer à l'action, mais aucun contrôle n'a été mis en place ou les contrôles qui l'ont été sont inefficaces et n'empêchent ni ne réduisent l'exploitation réussie de la vulnérabilité.	5

NIVEAU D'IMPACT	DESCRIPTION DE L'IMPACT	NOTE (NUMÉRIQUE)
Très faible impact (1)	Un événement représentant une menace peut avoir un effet négatif presque inexistant sur les opérations de l'entreprise, ses capacités à remplir sa mission, les actifs, les individus, les clients ou d'autres entreprises.	1
Faible impact (2)	Un événement représentant une menace peut avoir un effet négatif limité, c'est-à-dire : une dégradation des capacités du système à remplir sa mission, mais les fonctions primaires peuvent encore être exécutées ; des dommages mineurs ; des pertes financières mineures ; ou alors, les effets sont limités à certaines ressources cybernétiques sans toucher des ressources essentielles.	2
Impact moyen (3)	Un événement représentant une menace peut avoir un effet négatif significatif, c'est-à-dire : une dégradation marquée des capacités du système à remplir sa mission, mais les fonctions primaires peuvent encore être exécutées ; des dommages mineurs ; des pertes financières mineures ; ou alors, les effets sont marqués pour certaines ressources cybernétiques et essentielles.	3
Impact élevé (4)	Un événement représentant une menace peut avoir un effet négatif grave ou catastrophique, c'est-à-dire : une dégradation grave ou une perte des capacités du système à remplir sa mission, avec une ou plusieurs fonctions primaires ne pouvant plus être exécutées ; des dommages majeurs ; des pertes financières majeures ; ou alors, les effets s'étendent à la plupart des ressources cybernétiques et essentielles.	4
Impact très élevé (5)	On peut s'attendre à ce qu'un événement représentant une menace ait de multiples effets négatifs graves ou catastrophiques sur les activités et les biens de l'entreprise, sur les individus, sur d'autres entreprises ou sur les intérêts vitaux de la Nation. L'éventail des effets est vaste et concerne presque toutes les cyber-ressources.	5