



Octobre 2024

Recommandations quant aux contrôles de sécurité relatifs aux personnes dans les entreprises

1 Introduction

Dans le monde des affaires actuel, il est essentiel de pouvoir compter sur un personnel intègre et digne de confiance. Les entreprises ont la possibilité de diminuer les risques en effectuant des contrôles approfondis visant à garantir que seules les personnes dignes de confiance aient accès aux données sensibles, aux ressources financières ou aux systèmes critiques.

L'objectif de ces contrôles est de s'assurer que les personnes évaluées ne représentent aucun risque pour la sécurité. Il ne doit y avoir aucun doute quant à leur intégrité, à leur crédibilité et à leur fiabilité. Les circonstances de leur existence ne doivent pas les exposer au chantage ou à la corruption.

Les conditions dans lesquelles ce contrôle doit être réalisé et les conséquences d'une déclaration de risque doivent être clairement énoncées lors du processus d'engagement et dans le contrat de travail. Les exigences de la loi fédérale du 25 décembre 2024 sur la protection des données¹ doivent également être respectées.

Les présentes recommandations indiquent quels éléments sont pertinents pour l'analyse et comment les évaluer. Elles ont pour objectif d'aider les entreprises à effectuer de tels contrôles dans le cadre des exigences relatives à la gestion de la conformité, notamment les industries électriques ou gazières qui doivent assurer une sécurité informatique minimale².

¹ [Loi fédérale sur la protection des données](#), LPD ; RS 235.1.

² Dans son [ordonnance du 14 mars 2008 sur l'approvisionnement en électricité](#), OApEI ; RS 734.71, le Conseil fédéral a fixé la [norme minimale TIC](#) que doivent mettre en œuvre les entreprises des catégories A et B des secteurs de l'électricité et du gaz. Cela comprend notamment le devoir de soumettre les titulaires de certaines fonctions à des contrôles de sécurité (cf. [norme minimale pour améliorer la résilience informatique](#), Version 1.1, activité : PR.IP-11 ou NIST Cyber Security Framework 2.0, la fonction GV.PR-04).

2 Éléments contrôlés et évaluation

Le contrôle de sécurité comprend plusieurs démarches telles que la vérification de l'identité et la consultation de divers registres. Pour obtenir une image complète de la fiabilité de la personne contrôlée, les vérifications peuvent aussi s'étendre à son entourage personnel. Les mesures décrites ci-après permettent d'évaluer la situation de manière pertinente.

Éléments contrôlés	But du contrôle et étendue de la vérification
Casier judiciaire	<p>L'extrait de casier judiciaire ne doit comporter aucune mention de nature à faire douter de la fiabilité de la personne contrôlée.</p> <p>Il est possible de demander à celle-ci de présenter (volontairement) dans leur intégralité les jugements et les ordonnances pénales qui paraissent problématiques afin de les examiner de plus près.</p>
Registre des poursuites	<p>L'extrait du registre des poursuites ne doit comporter aucune mention susceptible de faire craindre un risque de corruptibilité. En déclarant qu'elle a des dettes et en expliquant comment elle compte les rembourser, la personne contrôlée peut contribuer favorablement à l'évaluation de son extrait.</p> <p>Elle doit être informée du fait qu'elle peut (volontairement) s'exprimer en détail sur d'éventuelles inscriptions abusives.</p>
Médias sociaux et Internet	<p>Il est également possible de consulter des sources publiques, notamment Internet et les réseaux sociaux, pour savoir si la personne contrôlée a pris part à des événements inappropriés ou si elle a diffusé des publications susceptibles de mettre son intégrité ou sa loyauté en doute, ou encore de l'exposer à un risque de corruptibilité.</p>
Diplômes et certificats	<p>La vérification des diplômes auprès des institutions qui les ont établis permet d'en vérifier l'exactitude. D'éventuelles falsifications indiquent que la personne contrôlée manque d'intégrité et qu'elle n'est pas digne de confiance.</p>
Liens avec l'étranger	<p>Des origines étrangères ou un séjour prolongé dans un autre pays peuvent entraîner le risque qu'un État tiers exerce une influence ou se livre à une tentative d'extorsion sur la personne contrôlée (p. ex. en menaçant sa famille sur place). Il est donc nécessaire d'évaluer si cette personne est digne de confiance.</p> <p>Dans le cas où, faute d'accord international suffisant ou faute de temps, il n'est pas possible de contrôler la situation des personnes étrangères, l'entreprise peut assumer ce risque ; elle doit alors le mentionner dans le processus de gestion du risque.</p>
Certificats de travail et employeurs	<p>De fausses indications sur les employeurs précédents ou sur les motifs de résiliation du contrat de travail peuvent indiquer que la personne contrôlée manque d'intégrité et n'est pas digne de confiance. C'est la raison pour laquelle il y a lieu de</p>

	prendre contact avec les précédents employeurs pour vérifier le fait que la personne ait bien travaillé à cet endroit, la teneur de son certificat de travail et les raisons pour lesquelles le contrat a été résilié.
Entretiens	Des entretiens permettent de passer tous les points précités en revue.

3 Les contrôles de sécurité font partie des processus organisationnels

- **Candidature** : le remplissage du formulaire de déclaration d'acceptation d'un contrôle de sécurité doit faire partie intégrante de la procédure et la personne qui présente sa candidature doit en être informée.
- **Procédure de contrôle de sécurité *a posteriori*** : lorsqu'une personne doit, après avoir été engagée, se soumettre à un contrôle de sécurité en raison de l'attribution de nouvelles tâches, son contrat de travail doit être adapté en conséquence.
- **Répétition de la procédure de contrôle de sécurité** : il y a lieu de répéter le contrôle de sécurité à chaque changement de fonction et, selon le degré de sensibilité des mandats, tous les deux à cinq ans. Nous recommandons aux employeurs de fournir spontanément tous les extraits requis par ces contrôles successifs afin de simplifier la procédure.
- **Critères de contrôle** : l'entreprise doit préciser ce qui doit être considéré comme critique s'agissant des extraits du casier judiciaire et du registre des poursuites, et élaborer un processus d'examen et de décision en ce sens. Dans la mesure du possible, les décisions et les entretiens doivent se dérouler selon le principe des quatre yeux afin d'augmenter la qualité de l'appréciation.
- **Classement des résultats et protection des données** : le contrôle et le classement des résultats doivent respecter les exigences de la loi sur la protection des données. Les informations qui n'ont plus aucune pertinence après que la décision a été rendue doivent être immédiatement effacées. Si le contrôle de sécurité est réalisé par un service externe, il convient de vérifier que celui-ci respecte les règles de la protection des données lors des échanges d'informations et du classement des données, et de documenter ces vérifications.
- **Registre du personnel** : ce registre doit indiquer les personnes qui doivent faire l'objet d'un contrôle de sécurité en raison de la nature des tâches qu'elles effectuent, de leurs droits d'accès et de leur fonction et préciser si ce contrôle a déjà été réalisé. La nécessité d'un contrôle dépend du degré de sensibilité des tâches et du dommage potentiel que la personne pourrait infliger à l'entreprise.
- **Livraisons effectuées par des fournisseurs externes** : le personnel des fournisseurs externes doit être intégré dans le processus. Il peut être obligé par contrat à se soumettre à un contrôle de sécurité (si une telle obligation fait défaut, il y a lieu de le mentionner dans le processus de gestion du risque).

4 Abréviations

CSF	Cyber Security Framework
DDPS	Département de la défense, de la protection de la population et des sports
ISO	Organisation internationale de normalisation
LSI	Loi sur la sécurité de l'information
NIST	National Institute of Standards and Technology
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFCS	Office fédéral de la cybersécurité
OFEN	Office fédéral de l'énergie