La certification, un vecteur de confiance adapté aux multiples enjeux du numérique

Arthur RIBEMONT
Responsable du Pôle Confiance Numérique
AFNOR Certification

Incertitude et besoin de confiance

Les crises se multiplient. COVID, climat, guerres, inflation : il est extrêmement difficile dans ce contexte pour une entreprise de pouvoir planifier faute d'une vision claire. Elles doivent faire face à de nombreuses incertitudes et cela pourrait impacter leur chaîne de valeur. Ces difficultés ne sont pourtant pas les seules auxquelles elles font face. Le risque numérique est incontournable comme le démontre de nombreuses études et baromètres dont celui d'Allianz - AGCS qui fait du risque cyber la 3e source d'inquiétude pour les chefs d'entreprise[1]. Sécuriser son activité dans ce contexte devient fondamental. Pour cela, il est nécessaire de réduire le risque en minimisant les aléas quand cela est possible. Dans une chaîne de valeur, les partenaires qu'ils soient sous-traitants, fournisseurs, distributeurs, etc. ont une place importante. S'appuyer sur des partenaires de confiance est essentiel ; pourtant cette dernière est intangible. La certification apparaît dans ce cadre comme un levier incontournable pour concrétiser cette confiance.

Qu'est-ce que la certification ?

La certification est la reconnaissance par une tierce partie qu'une entreprise, un produit, un service ou une personne est bien conforme à un ensemble de critères définis. La certification est une marque de garantie et son utilisation est encadrée par le code de la Consommation notamment pour ce qui concerne les produits et services. L'article L433-3 la définit comme suit : « *Constitue une certification de produit ou de service [..] l'activité par laquelle un organisme, distinct du fabricant, de l'importateur, du vendeur, du prestataire ou du client, atteste qu'un produit, un service ou une combinaison de produits et de services est conforme à des caractéristiques décrites dans un référentiel de certification.* ». L'article L433-5 précise *« Peuvent seuls procéder à la certification de produits ou de services les organismes qui bénéficient d'une accréditation ».*
Les deux précédents extraits illustrent trois aspects élémentaires d'une certification : le référentiel, l'audit et l'accréditation. Dans le cadre d'une certification, le référentiel ou règlement d'usage détermine un ensemble de critères auxquels doit se conformer l'organisme souhaitant obtenir une

[1] https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2021-fr.html

certification. La reconnaissance d'une certification, au niveau réglementaire et par le marché, nécessite que ses critères aient fait l'objet d'une concertation des parties intéressées. C'est notamment en France le rôle de l'AFNOR (Association française de normalisation) qui réunit au sein de commissions de normalisation, les parties intéressées pour obtenir un consensus sur les normes.

L'audit est l'étape incontournable d'un processus de certification. Celui-ci doit être réalisé par une tierce partie indépendante de l'organisme audité aussi appelé organisme certificateur. Après avoir déterminé le périmètre des activités à auditer, un premier audit documentaire est souvent réalisé pour déterminer la capacité de l'organisme à réaliser l'audit. S'en suit alors la visite sur site d'un auditeur compétent et qualifié qui va interroger les équipes, observer les pratiques et étudier les pièces documentaires. Un rapport est ensuite remis à un expert décisionnaire qui peut rendre un avis favorable ou non sur la délivrance de la certification.

Légitimité et impartialité

L'accréditation complète ce triptyque de la certification et permet à un organisme certificateur de délivrer des certifications. En France, le Cofrac (Comité français d'accréditation) est l'instance nationale désignée et reconnue par l'Etat pour attester des compétences d'un organisme de contrôle que sont les organismes certificateurs. Ces contrôles sont réalisés sur la base de normes, référentiels ou réglementations en vigueur. L'accréditation démontre le savoir-faire d'un organisme certificateur et apporte de la réassurance à l'audit réalisé par ce dernier.

Il est important de noter que lorsqu'un client manifeste sa volonté d'entrer dans une démarche de certification, il n'a aucune garantie quant à l'obtention de celle-ci. L'organisme certificateur est impartial. Pour résumer, AFNOR Certification définit la certification comme étant « *une preuve irréfutable, délivrée suite à un audit mené par un organisme certificateur impartial et objectif, qu'un produit, service ou une organisation, respecte les exigences d'un cahier des charges strict.* »

Quels sont les enjeux de la certification pour les organisations et personnes certifiés ?

Les enjeux de la certification peuvent être synthétisés en quatre grands axes : se conformer, conquérir, sécuriser et valoriser. Dans le cadre de certains marchés, la certification est obligatoire. C'est le cas par exemple des hébergeurs de données de santé qui doivent être certifiés selon le Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel. La seconde motivation est d'ordre commerciale et notamment de pouvoir concourir à des appels d'offres. Et la tendance est à la généralisation de telles pratiques.

Le troisième aspect concerne la sécurité de l'entreprise. La certification permet de garantir que des mesures répondant à un ensemble de critères définis sont mises en œuvre. Cela génère de la réassurance vis-à-vis de ses partenaires économiques. Enfin la certification peut également être le moyen de valoriser et fédérer les équipes grâce à une reconnaissance. C'est la récompense de tout un travail collectif. S'interroger sur les raisons de l'acquisition d'un signe de confiance est important pour maintenir dans le temps l'engagement des équipes.

La certification comme marque de garantie présente bien des atouts. A ce titre, c'est un puissant instrument pour répondre aux nombreux défis induits par le numérique. Le champ d'action est vaste et presque sans limite et concerne tout à la fois : l'innovation et ses risques critiques de dérives, l'explosion de la cybermenace dans un contexte de décentralisation des SI, la protection des libertés

individuelles, la compétitivité des entreprises et bien d'autres encore. Panorama de ces enjeux illustrés par les certifications afférentes.

La certification, une réponse possible au défi technologique

Les innovations dans le numérique sont constantes et rapides. Certaines pouvant entraîner des dérives. Pour n'en citer qu'une : l'affaire Cambridge Analytica, du nom de l'entreprise qui a été accusée d'utiliser des données Facebook pour influencer l'élection américaine. Le risque de dérive est d'autant plus important que les sujets sont intangibles et non maîtrisés par la grande majorité des personnes. Pour accompagner ces innovations, la Commission européenne a notamment dans le cadre de l'intelligence artificielle (IA) proposé une approche par les risques. Les systèmes d'IA présentant un risque classé comme « inacceptable » seront interdits. Pour les autres niveaux risques, cette réglementation devrait imposer : le marquage CE.

Ce dernier ne peut être considéré comme une certification. Le marquage CE indique qu'un produit a été évalué conforme par son fabricant conformément à un ensemble d'exigences. Le marquage CE n'est toutefois pas une certification mais une attestation. L'évaluation peut être réalisée par le fabricant lui-même (déclaration de conformité) ou dans d'autres cas, il doit recourir à un organisme notifié. Dans ce dernier cas, la notification peut être considéré comme une accréditation et le marquage CE comme une certification. Son obtention peut être corrélée à des normes harmonisées.

Les normes harmonisées décrivent les spécifications techniques permettant éventuellement de pouvoir démontrer le respect des exigences technique de la législation européenne. Elles sont élaborées à la demande de la Commission européenne par une organisation européenne de normalisation. Pour une entreprise, être certifiée sur une norme harmonisée s'inscrit pleinement dans la démarche d'obtention du marquage CE associé. En la matière, la France par l'intermédiaire du Secrétariat général pour l'investissement (SGPI) a initié un grand défi, sous animation AFNOR : « Comment sécuriser, certifier et fiabiliser les systèmes qui ont recours à l'intelligence artificielle ? ». Toutes ces démarches visent à instaurer un cadre de confiance.

La certification, un enjeu de sécurité et de souveraineté

Pour des enjeux politiques, comme celui de la souveraineté, la certification est également présentée comme un critère de garanti notamment pour les infrastructures critiques. C'est tout l'intérêt de la qualification SecNumCloud de l'ANSSI qui est au cœur de la stratégie du cloud de confiance. A fin septembre 2022, seules cinq entreprises ont obtenu cette qualification de très haut niveau[2]. Toutefois, la stratégie du gouvernement, et notamment les aides proposées par l'Etat, devrait encourager la mise en conformité des industriels.

Ce référentiel est construit sur la même base que l'annexe A « Objectifs et mesures » de la norme ISO/IEC 27001 - Management de la sécurité de l'information. La certification ISO/IEC 27001 est l'une des certifications les plus recherchées et demandées par les entreprises. La dernière étude de l'ISO Survey parue en 2022 révèle une accélération de la croissance du nombre de certifiés 27001 en France de près de 55% en 1 an (606 en 2021 vs 392 en 2020).

De nombreux autres signes de reconnaissance comme les certifications HDS – Hébergeur de données de santé, NF Service - systèmes d'archivage

[2] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf

électronique ou encore TISAX dédiée à l'industrie automobile s'appuient sur cette norme de référence. Ce standard pourrait prochainement devenir un incontournable pour toutes les entreprises. Initier dès à présent une démarche de certification pourrait être à court terme un avantage compétitif significatif pour les entreprises.

Et cela pourrait rapidement arriver. Dans un récent discours dédié au cloud de confiance, le Ministre de l'Economie et des Finances, Bruno Lemaire, a avancé la possibilité d'une certification pour les industriels ne sécurisant pas assez leurs infrastructures : « *Et je pense qu'il faut d'abord partir sur une base volontaire. Mais je le dis avec beaucoup de gravité, si jamais nos entreprises qui ont des données extraordinairement sensibles ne se saisissaient pas librement de cette offre de sécurisation de leurs données, je ne peux pas exclure que, à un moment ou à un autre, nous en venions à une norme obligatoire pour protéger notre souveraineté industrielle et protéger notre indépendance.* ».

La certification, un vecteur de réassurance pour ses partenaires économiques

Cette déclaration du Ministre s'inscrit dans un contexte où la menace cyber explose. La question n'est plus de savoir si une entreprise va être attaquée, mais quand. Dans son rapport d'activité 2021, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) recense 1057 incidents vs 759 incidents en 2020 (+40%). Parmi ces attaques, certaines sont orchestrées par rebond, utilisation d'un système intermédiaire pour attaquer un système. S'appuyer sur un partenaire non fiable peut contribuer à l'ouverture d'une brèche même au sein d'un système d'information sécurisé et les conséquences peuvent être importantes pour l'entreprise. A ce titre, la certification telle que l'ISO/IEC 27001 constitue un excellent vecteur de réassurance quant aux pratiques et mesures mises en œuvre au sein d'une organisation.

Autre domaine, même enjeux. Pour répondre aux enjeux de protection des données, le Règlement général sur la protection des données (RGPD) prévoit plusieurs mécanismes. De manière transverse, c'est-à-dire pouvant concerner presque tous les traitements, des certifications reconnues par les autorités compétentes ayant une portée nationale et/ou européenne commencent à apparaître sur le marché. Ces certifications peuvent être complétées sectoriellement par des codes de conduite visant à contrôler des traitements réalisés dans un cadre spécifique comme par exemple le CISPE dédiés aux fournisseurs de services d'infrastructure cloud (IaaS). Ces instruments volontaires parmi d'autres concourent à une meilleure prise en main de la conformité RGPD par les responsables de traitement et sont encouragés par la CNIL[3].

La dynamique de la certification à travers quelques exemples

Tous ces exemples montrent que la certification est un mécanisme important sinon incontournable au sein de l'Union européenne et que son utilisation tend à augmenter au fil des ans tant les enjeux dans le secteur numérique sont divers et complexes. Les travaux en cours, dans le cadre du règlement sur la cybersécurité [4], pour créer des schémas de certification européens sur le cloud (EUCS), les produits (EUCC) et la 5G (EU5G) sont autant d'indicateurs de cette tendance. Point intéressant à noter pour les industriels, les travaux initiés dans le cadre de EUCS visent une harmonisation des

[3] https://www.cnil.fr/fr/la-cnil-publie-son-plan-strategique-2022-2024

[4] Règlement (UE) 2019/881 - relatif à l'ENISA […] et à la certification de cybersécurité des technologies de l'information et des communications

certifications nationales comme SecNumCloud en France ou C5 en Allemagne.

L'ensemble de ces certifications ou équivalents, initiés par des acteurs de référence légitime concourent à créer un numérique de confiance pour les entreprises, les consommateurs et les citoyens. Loin de refléter toute la dynamique sur le sujet, elles sont représentatives de la dynamique actuelle. L'ANSSI propose par exemple des solutions à destination des prestataires de vérification d'identité (PVID), Cybermalveillance.gouv.fr valorise les professionnels en sécurité numérique grâce au label ExpertCyber. Le ministère de la Justice a développé Certilis, la marque de garantie pour les plateformes de résolution des litiges en ligne : conciliation, médiation et arbitrage. Enfin d'autres projets sont en discussion ou en attente de décret d'application comme la certification concernant les logiciels de contrôle parental ou la certification de cybersécurité des plateformes numériques destinée au grand public.

Quel futur pour la certification dans le domaine du numérique ?

Déjà nombreux, les sujets liés au numérique ne devraient pas manquer dans les années à venir : metavers, edge computing, web3, quantique, NFT, industrie 4.0, etc. Les besoins de sécurité et de réassurance vont plus que jamais être nécessaires. Dans un tel environnement, marqué par de nouvelles pratiques de travail (télétravail, cloud, etc.) et l'explosion des cybermenaces : la confiance est un élément incontournable et en constante progression dans les relations inter-entreprises. De par ces caractéristiques, la certification dispose de solides arguments pour accompagner l'essor de cette confiance. Elle apporte des garanties et un levier de différenciation aux acteurs qui y recourent.

En France la dynamique autour de la certification ISO/IEC 27001 est particulièrement intéressante. Couplée à une politique publique ambitieuse en matière de sécurité et résilience des entreprises françaises, ce standard de la confiance numérique pourrait contribuer à renforcer l'attractivité des entreprises françaises en Europe et à l'international. Tout en contribuant à faire de la cybersécurité un axe majeur de notre souveraineté numérique.

Pour faire face aux défis réglementaires, politiques ou encore technologiques, la certification apparaît comme une marque de garantie incontournable. Pour autant, la multiplicité des signes de reconnaissance non encadrés induisant des informations contradictoires aussi bien pour les consommateurs que pour les entreprises pourrait être préjudiciable et mener à la défiance des consommateurs. C'est ce que rappelle un récent rapport d'information du Sénat : « *Labels, scores, allégations, mentions valorisantes, informations obligatoires, simple marketing : la profusion semble mener à la confusion.* » [5] . Ne pas briser cette confiance, tel est l'enjeu de la certification pour les années à venir.

[5] http://www.senat.fr/notice-rapport/2021/r21-742-notice.html