Guide

LE PARCOURS PROGRESSIF EN CONFIANCE NUMÉRIQUE

→ SUIVEZ LE GUIDE

afnor CERTIFICATION

Comment préparer son organisation à la complexité de l'univers numérique ?

SOMMAIRE

AVANT-PROPOS

Au cœur de toutes les interactions aussi bien humaines que financières, il y a un principe immuable : la confiance. Cette confiance est essentielle pour mener à bien un projet.

Une organisation produisant des biens ou des services en a besoin pour attirer ses clients et développer son activité.

La confiance est partout. Dans les relations humaines avec ses équipes et collaborateurs, les relations financières avec ses créanciers et clients, les relations commerciales avec ses partenaires et prestataires, etc. Ces liens de confiance sont essentiels et pourtant, ils sont quasiment intangibles. Ils dépendent des affinités entre partenaires, de leur réputation et de leur crédibilité sur le marché ainsi que des instincts et intuitions de chacun.

Aussi, l'une des missions d'AFNOR Certification est de concrétiser cette confiance.

Déjà très présent dans de nombreux domaines comme la qualité, la sécurité et l'environnement, AFNOR Certification se renforce en développant son offre en matière de cybersécurité et prolonge cet accompagnement dans l'univers numérique.

Acquérir un système de management mature requiert du temps. Et cela est d'autant plus vrai dans le numérique que les tendances et usages évoluent rapidement. Protéger ses données et sécuriser son patrimoine informationnel doit se faire à travers le temps et en continu. C'est pourquoi ces démarches doivent pleinement s'intégrer au cœur de la culture de l'entreprise pour être efficaces et efficientes.

Avec un parcours progressif et au rythme des entreprises, AFNOR Certification permet à chaque organisation d'acquérir la confiance nécessaire à son développement économique. Ce guide vise aussi à illustrer cette démarche au travers d'exemples concrets en matière de transformation numérique, cybersécurité et de protection des données.

Bonne lecture

UN UNIVERS À HAUT RISQUE

En quelques décennies, la société s'est métamorphosée.

La dépendance au numérique était déjà mise en avant en 2017 par BPI France[1]. L'organisme alertait qu'une entreprise sur cinq serait vouée à disparaître si elle n'opérait pas une profonde transformation numérique.

Si certains doutaient encore de l'importance prise par le numérique au quotidien : la crise sanitaire de la COVID-19 l'a confirmé. Grâce à Internet, aux services de visio-conférence, aux services en ligne hébergés dans le cloud ou encore aux e-mails sur le cloud, les entreprises ont pu maintenir leurs activités malgré les confinements successifs.

En 2020 et de surcroît en 2021, la situation démontre plus que jamais cette nécessité.

Le numérique est devenu incontournable. Avec son lot de bénéfices et de désagréments.

Chaque jour de nouvelles entreprises sont victimes d'agissements malveillants de la part d'entités concurrentes ou criminelles. Le cyberespace n'est pas un simple espace commercial. C'est un environnement où se côtoient les activités d'espionnage et les activités militaires des Etats. Dans cet univers, les frontières sont pratiquement inexistantes.

Toute entreprise est une cible potentielle. Dûment choisie ou inopinément attaquée. Obligeant ainsi chacune d'entre elles à se protéger et anticiper les menaces. Pourtant malgré toutes les protections mises en place : aucune ne pourra se prémunir totalement contre un clic par inadvertance sur une pièce jointe ou une URL corrompue.

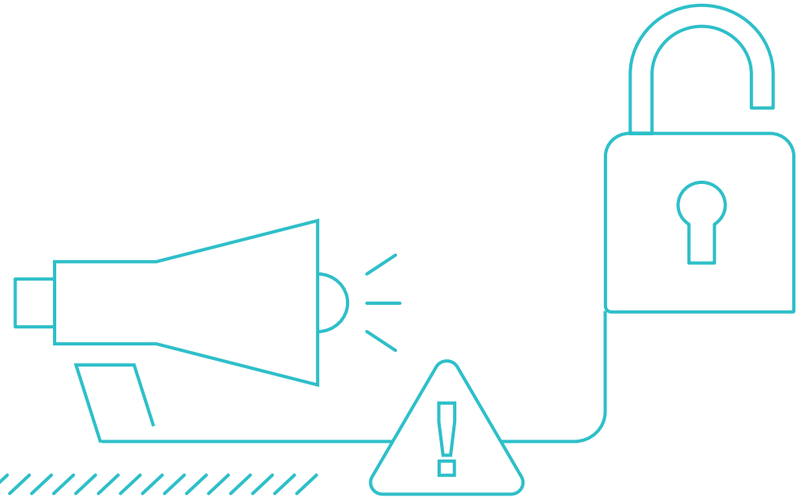
Pour ces raisons, savoir se préparer en se posant les bonnes questions est déterminant. A travers trois parties mêlant à la fois contexte et solutions, ce guide illustre le parcours proposé par AFNOR Certification pour comprendre et acquérir les bases d'un système de management de la confiance numérique.

Chaque partie peut être lue de manière indépendante. L'ensemble permet de découvrir les piliers de la confiance numérique. Ce guide aspire ainsi à donner du sens à cette notion de confiance si importante pour le développement des organisations dans un univers si opaque.

1

1 - Etude BpiFrance / LeLab 2017 - https://lelab.bpifrance.fr/content/download/750/file/Etude_DirigeantsfaceaudigitalBpifranceLeLab.pdf?version=1

I - LA DÉCOUVERTE



LA TRANSFORMATION NUMÉRIQUE PAR LE PRISME DES ENJEUX

La crise sanitaire a été un accélérateur de la digitalisation. Certaines organisations étaient prêtes. D'autres ont dû s'adapter à marche forcée pour maintenir leurs activités. La généralisation du télétravail a été un défi pour bon nombre d'entreprises ainsi qu'une source de vulnérabilité supplémentaire.

Ces vulnérabilités sont parfois sans conséquences. Lorsqu'un individu s'invite dans une réunion en visioconférence, c'est dérangeant mais il peut très vite être repéré et exclu. En revanche, cela devient plus critique si cette intrusion se passe dans le système d'information. La repérer est plus délicat. Nettoyer le système peut requérir beaucoup de temps et d'abnégation.

En cas d'intrusion, l'activité peut être difficile à maintenir. Pour éviter ces problèmes, il est recommandé de prévenir ces incidents en préparant bien en amont cette transition. C'est une condition sine qua non de la satisfaction des clients.

Et cela d'autant plus qu'intégrer ces nouveaux usages demande une certaine organisation. Les parcours et les modes de production peuvent être transformés. La capacité opérationnelle et le bien-être des collaborateurs peuvent être affectés. Et il faut aussi veiller à maintenir les relations avec les fournisseurs et partenaires.

À ces impératifs opérationnels incontournables s'ajoutent d'autres écueils. L'univers numérique, encore comparé au Far-West dans les années 2000, a été profondément réglementé depuis. Pour exemple, les lois nationales dans l'Union européenne en matière de protection des données (Loi Informatique et Libertés en France) ont été renforcées par l'entrée en application, en 2018, du Règlement Général sur la Protection des Données (RGPD).

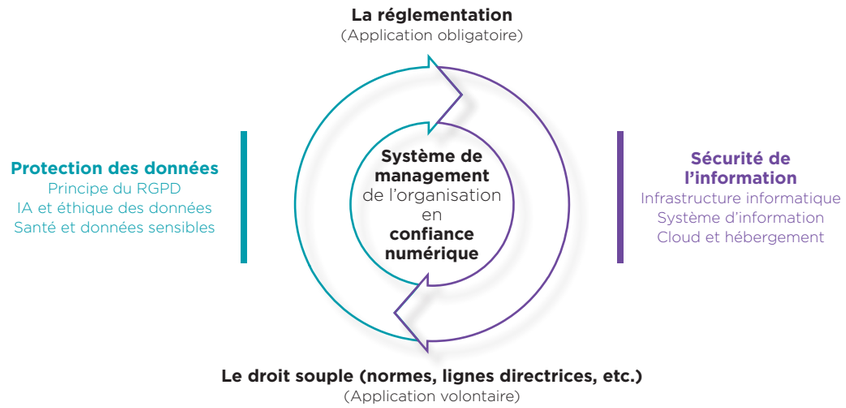
Dans les années à venir, cette règlementation déjà dense et complexe va s'intensifier. La Commission européenne étudie actuellement de nouveaux projets réglementaires visant à réguler les services numériques, harmoniser le marché européen ou encore encadrer les systèmes d'intelligence artificielle.

La non-identification et prise en compte de ces enjeux réglementaires pourrait porter préjudice aux organisations. D'une part d'un point de vue financier. Mais aussi et surtout en termes d'image auprès des clients et partenaires.

De la même manière, les incidents liés à une cyberattaque peuvent causer de profonds dommages. C'est devenu le risque numéro un des entreprises selon le baromètre des risques 2020 d'Allianz[1]. Début 2021, l'ANSSI révélait que le nombre de cyberattaques avaient explosé en 2020 (x4 par rapport à 2019)[2].

Ce tour d'horizon de l'univers numérique peut paraître intimidant. Certaines entreprises préfèrent occulter ces sujets pour ne pas complexifier leurs processus. Pourtant, les négliger peut coûter cher. Le coup d'arrêt porté à l'activité économique dans de tel cas ainsi que les dommages causés à la notoriété de l'organisation peuvent être irréversibles.

Bien se préparer permet d'atténuer ces risques. Dans cette optique, la définition d'une orientation, d'une stratégie et d'une feuille de route sont des pratiques recommandées pour y parvenir. Et ainsi amorcer un système de management en confiance numérique.



1 - Baromètre des risques 2020 d'Allianz
https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-fr.html

2 - Interview de Guillaume Poupard - directeur général de l'ANSSI sur BFM Business
https://www.bfmtv.com/economie/replay-emissions/le-grand-journal-de-l-eco/guillaume-poupard-anssi-le-nombre-de-cyberattaques-explose-en-2020-11-01_VN-202101110328.html

1

2

ÉVALUER SON NIVEAU DE MATURITÉ EN CONFIANCE NUMÉRIQUE

Des organismes comme l'ANSSI, la CNIL, le GIP ACYMA et bien d'autres publient régulièrement des supports pour accompagner les organisations dans ces démarches. Ces documents librement accessibles sur leur site web permettent de mieux appréhender l'univers numérique et les mesures à mettre en place pour protéger une organisation.

À titre d'exemple, l'ANSSI a publié un guide début 2021 destiné aux TPE/PME pour les aider dans leurs démarches de cybersécurité. Il permet d'identifier 12 pistes d'attention parmi lesquelles la connaissance du parc informatique, la sécurisation des messageries ou encore les premiers gestes à effectuer en cas de cyberattaque[3].

Pour accompagner cette tendance, AFNOR Certification accompagnée par des experts, a élaboré les **focus cybersécurité et RPGD**. Réalisés sous forme de questionnaires simples et accessibles, ils permettent à une organisation de mesurer sans frais et librement son niveau de maturité. L'objectif est de délivrer un état du niveau de maturité des organisations en matière de protection des données (RGPD) et de sécurité de l'information (cybersécurité) ; deux des piliers de la confiance numérique. Dans ce cadre, l'organisme est invité à apprécier son niveau en sélectionnant celui le plus proche de ceux proposés, à savoir de la non-connaissance du sujet à sa parfaite maîtrise.

À l'issue du questionnaire, un rapport complet et illustré est généré. Il synthétise les points forts et les axes de progrès de l'organisation. Ces éléments sont regroupés au travers de trois grandes thématiques : opérationnelle, ressources/pilotage et leadership permettant à l'organisation de structurer sa feuille de route.

2 questionnaires

- **Cyber :** 44 questions dont 1 éventuellement non applicable («Conception de logiciels»)
- **RGPD :** 38 questions dont 1 éventuellement non applicable («Encadrement des transferts de DCP»)

3 thèmes

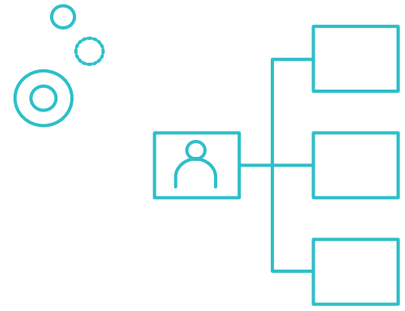
- **Partie opérationnelle :** Fonctionnement et support opérationnel (1/3 du questionnaire)
- **Ressources/pilotage :** Ressources et moyens (1/3 du questionnaire)
- **Leadership :** Leadership gouvernance et stratégie (1/3 du questionnaire)

4 niveaux de réponse

- **Je ne connais pas** ou je n'en ai aucune idée
- Sujet identifié mais **plan d'action non défini**
- Sujet identifié et **en cours de traitement**
- Sujet **parfaitement maîtrisé** par mon organisation

3

3 - https://www.ssi.gouv.fr/uploads/2021/02/anssi-guide-tpe_pme.pdf

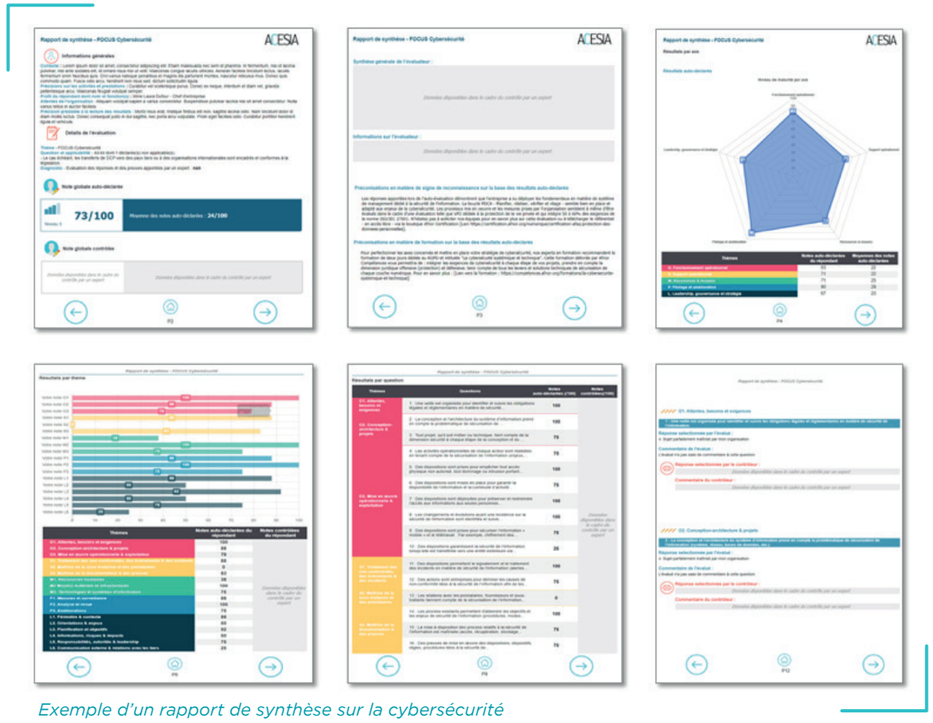


Indiquer maîtriser un sujet est une bonne chose. **Encore faut-il pouvoir le prouver.** Que ce soit dans le cadre d'un audit, d'un contrôle ou tout simplement pour les collaborateurs de votre organisation (et en particulier en cas de turnover élevé) : **il est important d'avoir une preuve formelle des processus, méthodes et bonnes pratiques pour faciliter leur transmission.**

Demandez-vous où trouver ces informations lorsque vous réaliserez votre auto-évaluation ☺.

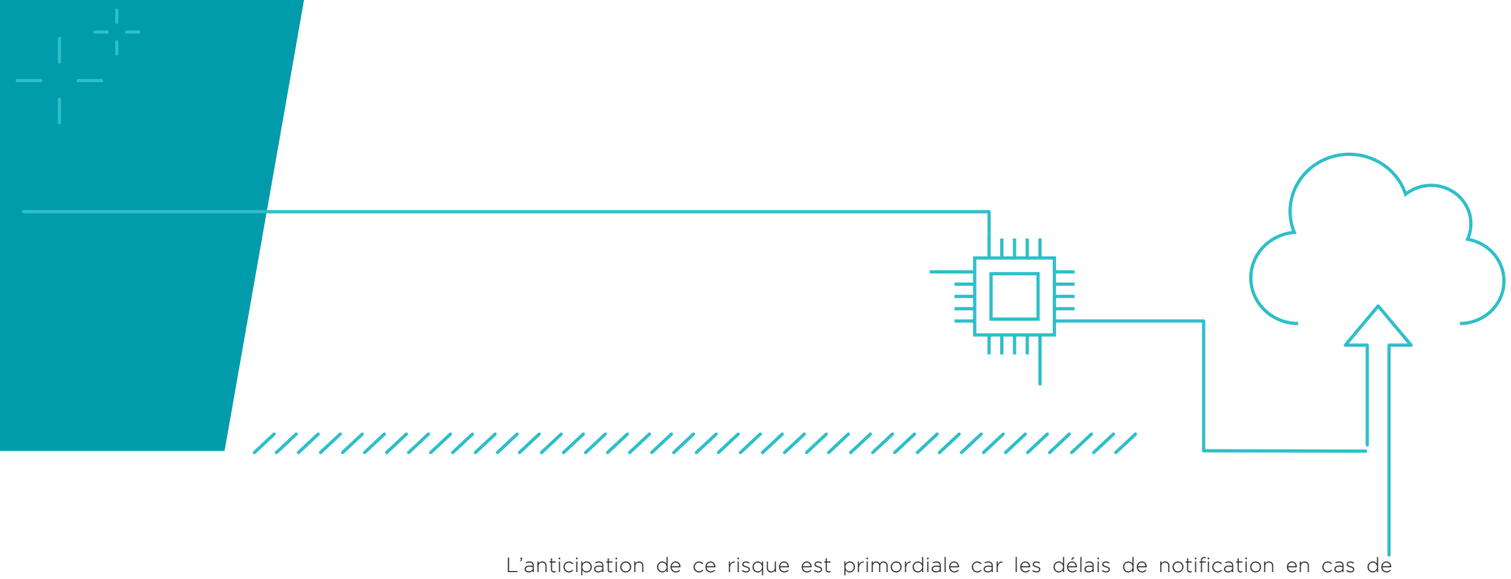
Les organisations souhaitant aller plus loin pour questionner leur niveau de maturité peuvent solliciter un diagnostic. Un expert sera alors missionné par AFNOR Certification pour évaluer la pertinence entre les déclarations et les preuves apportées. Il posera un regard critique s'agissant des mesures transmises par l'organisation.

Pour accompagner l'organisation, des formations et des signes de reconnaissances seront préconisés selon le niveau déclaré et contrôlé. La confiance numérique étant l'affaire de tous, AFNOR Certification propose une offre dédiée, sous certaines conditions, aux organisations souhaitant faire évaluer leurs fournisseurs ou leurs partenaires.



Exemple d'un rapport de synthèse sur la cybersécurité

II - LA VALORISATION



LA PROTECTION DE LA VIE PRIVÉE PAR LE PRISME DE LA NOTIFICATION EN RÉPONSE À UN INCIDENT

Comme cela a été vu dans le premier chapitre, l'enjeu de la protection des données a pris une toute autre ampleur avec le RGPD. Ce texte a renforcé les droits des citoyens et les devoirs des organisations traitant des données personnelles tout en renforçant les sanctions en cas de manquement à ces règles.

Les obligations sont nombreuses tout au long du cycle de traitement des données : registre de traitements, analyse d'impact, conservation des preuves, réponses aux droits des personnes, etc. Les grands principes tels que la détermination des finalités ou la minimisation des données doivent être intégrés dès la conception et par défaut (*privacy-by-design et privacy-by-default*).

Ces principes sont pour certains difficiles à appréhender et à mettre en œuvre. C'est pourquoi, le Comité européen pour la protection des données personnelles (CEDP ou EDPB) publie régulièrement des lignes directrices, des recommandations et des bonnes pratiques visant à clarifier ces principes et accompagner les responsables de traitement et sous-traitants.

En 2021, le CEDP a par exemple publié un projet de lignes directrices concernant la gestion des notifications en cas de violation des données personnelles[1]. Ce document recense un ensemble de bonnes pratiques, illustré par des exemples, pour savoir comment réagir et notifier les cas de violation de la sécurité des données.

Pour rappel, l'article 4.12 du RGPD précise ce qu'est une violation de la sécurité des données : « *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation [...] ou l'accès non autorisé à de telles données.* »

1

1 - https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf (Document en anglais)

L'anticipation de ce risque est primordiale car les délais de notification en cas de violation sont très courts. La notification à l'autorité compétente, la CNIL en France, doit être réalisée dans un délai de 72 heures comme le précise l'article 33 du RGPD.

Comme le rappelle la CNIL sur une page web dédiée aux violations de données personnelles[2], ces dispositions permettent à la fois de préserver le responsable de traitement et surtout les personnes affectées par la violation.

L'équivalent de la CNIL aux Pays-Bas (Dutch Data Protection - DPA) a récemment prononcé une sanction administrative de 475 000 € à l'encontre d'un grand site du secteur du tourisme. Le motif ? Avoir tardé à notifier une violation de données ayant concerné 4 000 personnes dont les données bancaires de près de 300 personnes[3].

Ce dernier exemple montre bien la nécessité de prévoir tous les scénarios y compris les plus difficiles. Car les sources de violations de données sont nombreuses et ne cessent de croître : cyberattaques, rançongiciels ou encore des négligences humaines. C'est pourquoi l'organisation doit prévoir la gestion de ces incidents afin de réagir rapidement en cas de survenance d'un tel événement.

ACQUÉRIR SON PREMIER SIGNE DE RECONNAISSANCE EN CONFIANCE NUMÉRIQUE

Dans l'univers numérique, où tout est dématérialisé, il est difficile d'apprécier la qualité des mesures déployées pour faire face à d'éventuels incidents. Et cela est d'autant plus critique sur un sujet aussi sensible que les données personnelles. D'où la nécessité de créer des labels de confiance ou signes de reconnaissance.

C'est dans cette optique qu'AFNOR Certification et un groupe d'experts ont développé le référentiel VP2 - Valoriser la protection de la vie privée. Pour l'obtenir, il est nécessaire de passer par une phase d'audit. Cette phase est à la fois exigeante en termes de préparation et rassurante pour les clients car neutre et impartiale.

2

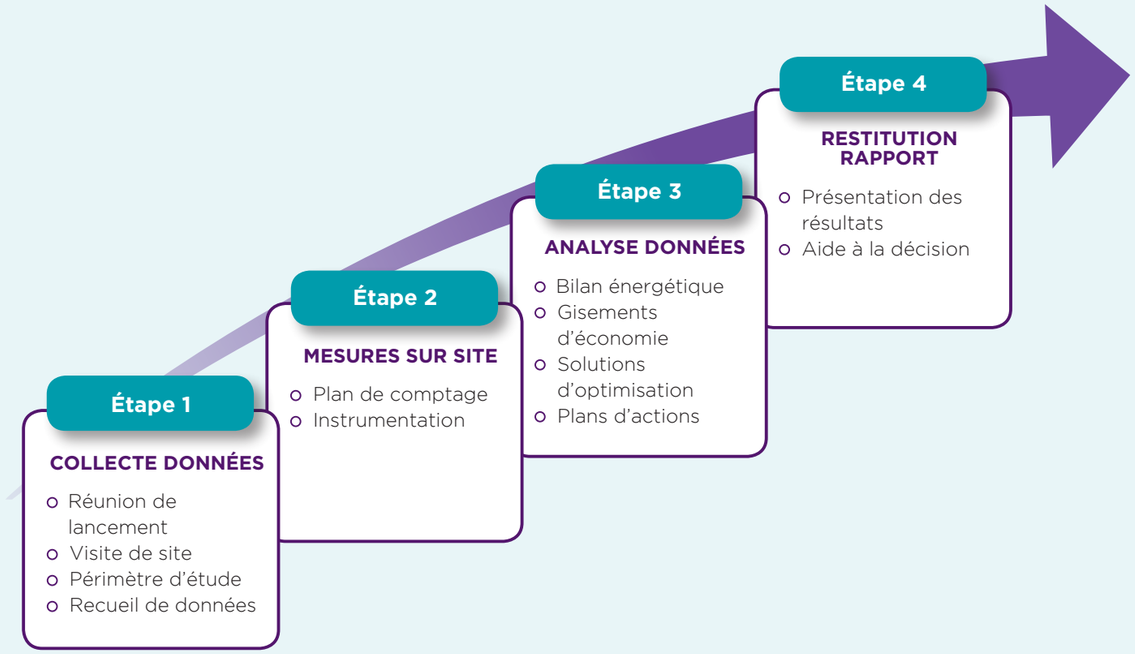
3

2 - https://www.cnil.fr/fr/les-violations-de-donnees-personnelles

3 - Pour en savoir plus sur les détails de cette sanction tombée en avril 2021 : https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-bookingcom-delay-reporting-data-breach_fr

L'audit classique

L'audit est particulièrement encadré et est composé de plusieurs étapes. La première étape permet une prise de contact entre l'équipe d'auditeurs/trices et l'organisation. Elle permet de s'assurer que tout est prêt. Elle est opérée trois à quatre semaines avant la date de l'audit. Laissant ainsi un temps pour les derniers ajustements.



Cette approche par l'audit est d'autant plus importante que le RGPD a profondément modifié les règles. Avant son entrée en application, traiter des données personnelles nécessitait une autorisation ou une déclaration auprès de la CNIL. Ces démarches ont été remplacées par une logique de responsabilité. En clair, l'organisation est responsable de la bonne application du RGPD et doit pouvoir le démontrer.

Cette logique de démonstration est au cœur de l'audit. Et en particulier de la seconde étape. C'est lors de celle-ci que l'équipe d'auditeurs/trices évalue en profondeur le fonctionnement général et les processus de l'organisation. Elle démarre par une réunion de présentation du plan d'audit et se termine par une restitution des constats réalisés au cours des observations, entretiens et examens documentaires.

Ces éléments sont consignés dans un rapport listant les non-conformités mineures et majeures, les points sensibles et de progrès et les notes de l'auditeur. C'est sur la base de ces éléments qu'un expert indépendant peut prendre la décision d'attribuer ou non un signe de reconnaissance comme VP2 à une organisation.

Cette démarche permet de valoriser les engagements pris par l'organisation en matière de protection des données personnelles et d'obtenir des engagements irréfragables de la part des sous-traitants. Cela est d'autant plus important que le principe de responsabilité s'applique aussi bien aux responsables de traitement, qui détermine les finalités et les moyens d'un traitement (article 5), qu'aux organisations ayant recours à de la sous-traitance (article 28).

Dans la continuité d'une décision favorable, l'organisation est contrôlée chaque année pour s'assurer que les mesures sont toujours pleinement opérationnelles. Ces audits de suivi permettent aussi de porter une attention particulière aux non-conformités mineures et points sensibles observés lors de ces précédentes visites. Au bout de trois ans, l'organisme redémarre un nouveau cycle d'audit.

Le référentiel VP2 apporte une réponse aux organisations souhaitant valoriser leur engagement en matière de protection des données personnelles. Il apporte des réponses à l'ensemble des obligations prévues par le RGPD, tout en s'appuyant sur les caractéristiques clés des systèmes de management comme l'ISO/IEC 27001 relatif à la sécurité de l'information.

AFNOR Certification a rassemblé des experts pour créer un signe de reconnaissance équivalent en matière de cybersécurité. Le principe étant de permettre à chaque organisation de valoriser le pilier de la confiance numérique, cybersécurité ou RGPD, qu'elle juge le plus opportun dans leur stratégie de conquête.

Les attendus de ces référentiels sont exigeants. Ils sont toutefois plus abordables que certaines certifications basées sur des normes par exemple. Ces signes de reconnaissance peuvent être une ambition et un objectif pour les plus petites structures alors qu'ils sont un point d'étape pour les organisations souhaitant accéder à la certification ISO/IEC 27001, ISO/IEC 27701 ou à toute autre certification équivalente.

III - L'EXCELLENCE

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION PAR LE PRISME DES RISQUES

Après avoir évoqué la gestion des incidents, il est à présent légitime de s'interroger sur le moyen de les éviter. Et de s'intéresser à l'anticipation des risques.

En premier lieu, il est important de noter que même si les niveaux de risque peuvent varier d'une entreprise à une autre, toutes les organisations font face à des risques qu'il est nécessaire d'identifier pour s'adapter et s'en protéger. Et le risque ne vient pas forcément de là où on l'attend.

Avec le numérique, tout est interconnecté au réseau. De fait un client ou un fournisseur infecté peut potentiellement nuire à l'activité, au développement ou à l'image. Le scandale SolarWinds[1] démontre bien que la menace peut venir de partout et qu'aucune organisation n'est à l'abri.

Anticiper et atténuer les risques, c'est permettre à l'organisation de mieux protéger son patrimoine informationnel - tout ce qui constitue la richesse de l'entreprise au quotidien (portefeuille clients) et pour le futur (nouveaux projets/produits) - ainsi que sa réputation et son image.

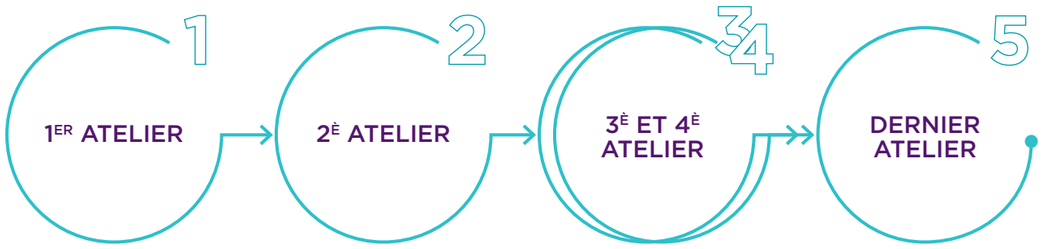
Pour atteindre ces objectifs, différentes méthodes existent. La méthode EBIOS propose une démarche itérative en 5 ateliers permettant d'apprécier et de traiter les risques numériques[2].

1 2

1 - https://www.nextinpact.com/article/46482/cyberespionnage-solarwinds-victimtotal-anti-virustotal

2 - https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

Schéma de la méthode EBIOS



Identifier le périmètre, les activités et les événements redoutés ainsi que leur niveau de criticité pour l'organisation.

Identifier les différentes sources de risques (Hacktivistes, concurrents, etc.) ainsi que les motivations et objectifs associés à telles actions permettant in fine de déterminer les risques à couvrir en priorité.

Décrire les potentiels chemins d'attaque à la fois d'un point de vue stratégique et opérationnel.

Mettre en oeuvre une stratégie en matière de traitement des risques.

Il existe de nombreuses autres méthodes permettant d'analyser et d'anticiper les risques comme par exemple la norme ISO/IEC 27005[3] ou encore MEHARI proposée par le Clusif[4]. À chaque organisation de trouver celle qui lui convient le mieux. Ces analyses permettent de déterminer les mesures de sécurité à mettre en œuvre.

3 4

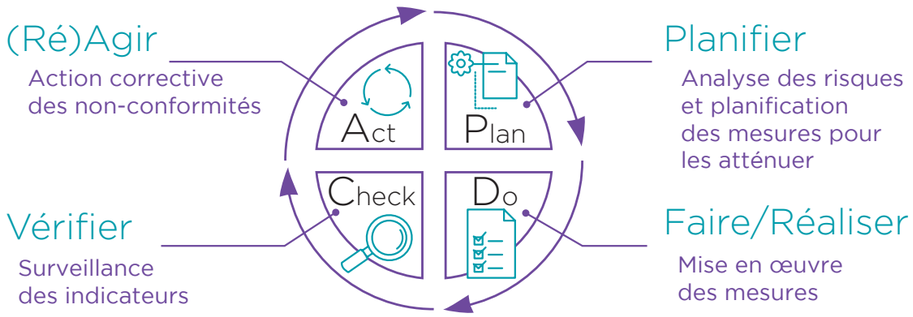
3 - https://www.boutique.afnor.org/norme/nf-iso-iec-27005/technologies-de-l-information-techniques-de-securite-gestion-des-risques-lies-a-la-securite-de-l-information/article/914089/fa193458

4 - https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari

> Anticiper,
> c'est se donner la capacité de réagir
> rapidement et efficacement.

Toutes les mesures prises pour prévenir les risques identifiés ne peuvent éviter la survenance de certains incidents. Elles permettent toutefois d'orchestrer plus rapidement une réaction coordonnée. Par ailleurs, la réalisation du retour d'expérience doit permettre de tirer les conclusions à même de faire évoluer les mesures de sécurité. Ainsi le système s'enrichit et devient plus résilient contre ce type de menace. Ce mécanisme appelé amélioration continue est l'un des principes clés du système de management.

Schéma simplifié d'un système de management
Boucle d'amélioration continue



DÉVELOPPER UNE VÉRITABLE CULTURE DE L'ANTICIPATION DES RISQUES

La mise en place d'un système de management est un gage de qualité de l'organisation. Et en matière de sécurité de l'information, **l'ISO/IEC 27001 est le système de management de référence** (aussi appelé SMSI pour système de management de la sécurité de l'information).

C'est un référentiel très exigeant qui est le fruit d'un travail intensif et collectif mené au niveau international par des experts de tous les pays. Sa légitimité vient du fait qu'il a fait l'objet d'un consensus de la part de l'ensemble de ces experts . *Pour en savoir plus :*
https://normalisation.afnor.org/foire-aux-questions/comment-est-elaboree-norme-volontaire/

Basé sur le management par les risques, ce référentiel permet de définir les orientations, enjeux et objectifs de l'organisation en matière de sécurité de l'information. La mise en œuvre de ce référentiel ne garantit pas une protection entière et systématique contre les cyberattaques. En revanche, bien appliqué, il permet d'atténuer le risque et favoriser une reprise d'activité rapide malgré les dégâts causés par un tel incident.

Cependant son intégration nécessite un certain savoir-faire. En effet, les systèmes de management « classiques » sont constitués d'une trentaine d'exigences. Celui de l'ISO/IEC comporte une annexe de 114 exigences supplémentaires à appliquer. Pour ces raisons, le recours à des professionnels est vivement recommandé.

Quelques grandes étapes sont incontournables dans la mise en place d'un SMSI :

1. La première consiste à déterminer un périmètre, afin d'identifier les enjeux internes et externes comme les aspects réglementaires et les parties intéressées, et les ambitions de l'organisation.

2. La deuxième grande étape repose sur la définition des rôles et responsabilités de chacun dans sa mise en place. L'une des clés est l'engagement de la direction et la définition d'objectifs clairs à atteindre. Sans cette implication, la légitimité du système sera probablement remise en cause. Au détriment de toute la stratégie de sécurisation de l'organisation.

3. S'ensuit la mise en place de l'analyse des risques et la détermination des mesures à prendre pour les atténuer. Il est alors nécessaire d'implémenter une à une l'ensemble des exigences du référentiel y compris toutes celles de son annexe. Enfin presque toutes. Certaines pourraient ne pas être pertinente auquel cas, il est possible de les exclure en le justifiant dans la déclaration d'applicabilité (DdA).

En parcourant ce chemin, l'entreprise a mis en place un système de management dit « jeune ». Pour atteindre une certaine maturité, il doit être éprouvé, c'est à dire parcourir le cycle du système de management à plusieurs reprises et ainsi développer un véritable savoir-faire en matière de sécurité de l'information. Développant ainsi un véritable savoir-faire en matière de sécurité de l'information.

Bien entendu ce cheminement vaut également pour la mise en place d'une stratégie efficace en matière de protection des données. Si certains aspects ne sont pas requis par le RGPD, le raisonnement général autour de l'amélioration continue constitue un atout indéniable pour la stratégie de l'entreprise.

Toutes les organisations souhaitant démontrer la conformité de leurs traitements de données personnelles, conformément à l'article 42 du RGPD pour les initiés, pourront prochainement en faire la demande auprès d'AFNOR Certification.

L'alliance combinée de ces approches permettra aux organisations d'attester d'un haut niveau de maîtrise des risques tant d'un point de vue du RGPD qu'en matière de cybersécurité.

LE PARCOURS PROGRESSIF

Tisser un lien de confiance avec ses clients et partenaires est essentiel pour la pérennité d'une activité. Le recours à des signes de confiance reconnus peut être un bon moyen de l'initier. Cependant acquérir de tels labels demande un certain savoir-faire. Des méthodes et du temps.

Ces difficultés peuvent être un frein. Pourtant, le numérique démontre jour après jour la nécessité de s'emparer pleinement des enjeux de cybersécurité et de protection des données. Et toutes les organisations sont concernées. Déployer des mesures et le faire-savoir est indispensable.

L'adoption d'une démarche progressive et adaptée facilite cette mise en œuvre. Le parcours progressif proposé par AFNOR Certification est un guide vers la confiance numérique conçu en trois phases.

La découverte illustre la nécessité d'évaluer les forces et faiblesses

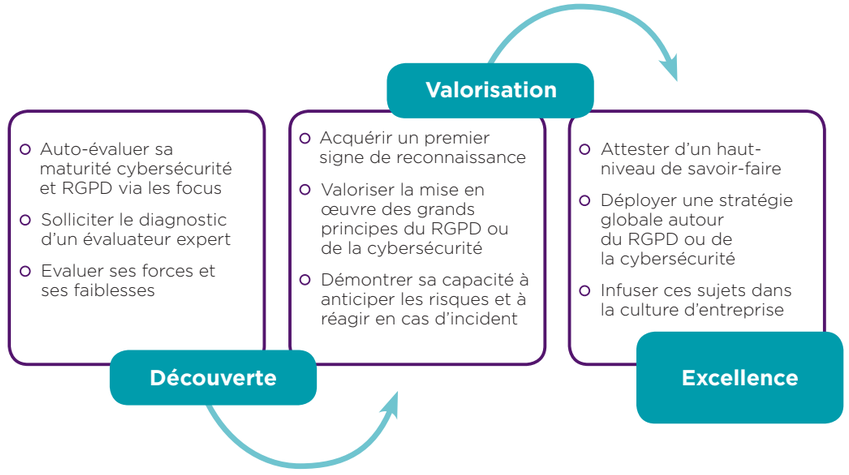
La valorisation démontre la capacité à réagir

L'excellence révèle une culture d'anticipation des risques

Pensé par le prisme de l'amélioration continue, ces étapes ont été développées pour apporter des réponses à tous les stades de maturité des organisations. Les focus, VP2 et l'ISO/IEC 27001 sont autant de solutions adaptées. Elles correspondent à des enjeux et des ambitions propres à chaque organisation.

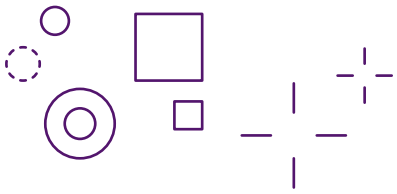
Grâce à la démarche proposée par AFNOR Certification, « restez focus » sur la satisfaction de vos clients tout en les rassurant sur votre capacité à faire face aux défis et enjeux du numérique.

Parcours progressif classique



POUR EN SAVOIR PLUS

certification@afnor.org
01 41 62 80 11



Communication Groupe AFNOR – S2108005 – 08/21 – Conception graphique : EMA.

afnor CERTIFICATION