CGI

La force de l'engagement[MD]

Comprendre les normes de cybersécurité

Avril 2019


information
protection
Shift

Introduction

Compte tenu des décisions capitales qui doivent être prises dans un environnement de cybermenaces en constante évolution, les normes de cybersécurité constituent pour les entreprises un moyen crucial de s'assurer que leur stratégie et leurs politiques de sécurité font l'objet d'une mise en œuvre cohérente et mesurable. Dans le présent document, nous décrivons le rôle des normes de cybersécurité dans le contexte général des technologies de l'information (TI) et proposons les meilleures pratiques à adopter pour établir un cadre de travail relatif aux normes de cybersécurité et gérer la conformité. Bien que ce document mette l'accent sur les normes de sécurité des TI et de confidentialité, les normes de sécurité physique jouent également un rôle parallèle important. De nombreux principes de base décrits dans ce document peuvent également s'appliquer à la sécurité physique.

Le présent document décrit le rôle des normes de cybersécurité dans le contexte général des technologies de l'information (TI) et propose les meilleures pratiques à adopter pour établir un cadre de travail relatif aux normes de cybersécurité et gérer la conformité.

Qu’est-ce qu’une norme de cybersécurité?

Selon le dictionnaire Oxford, une norme est un « niveau de qualité ou de réalisation ». En ce qui concerne les normes de cybersécurité, la définition ci-dessous propose plusieurs principes utiles.

Les normes de cybersécurité peuvent être définies comme les moyens essentiels par lesquels l’orientation décrite dans la stratégie et les politiques de cybersécurité d’une entreprise est transformée en critères exploitables et mesurables.

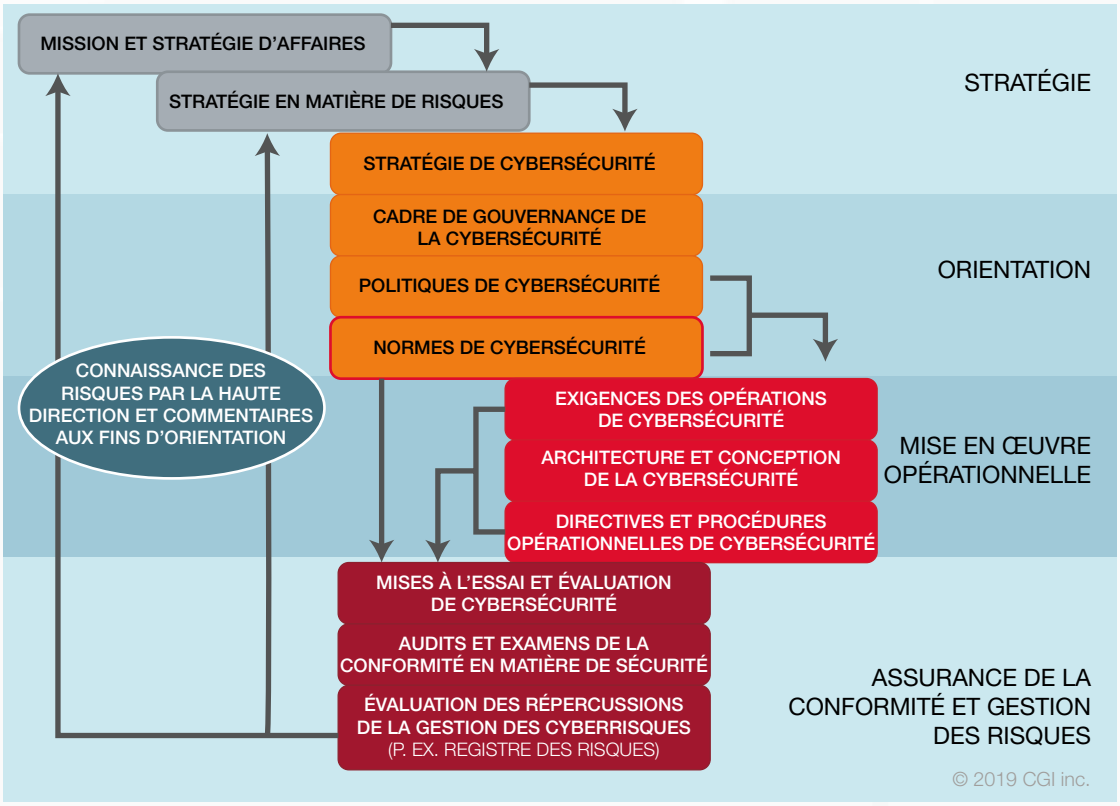
Les normes de cybersécurité sont des énoncés qui décrivent les résultats que l’entreprise doit obtenir pour atteindre ses objectifs en matière de sécurité. La façon dont les normes doivent être mises en œuvre et les solutions à adopter pour les respecter ne font pas partie des normes proprement dites. Ces renseignements doivent plutôt figurer dans les plans et les procédures opérationnelles élaborés pour appliquer les normes le moment venu.

Normes de cybersécurité et gouvernance des TI

Les normes de cybersécurité représentent une étape clé du processus de gouvernance des TI. Pour gérer les risques et les limiter à des niveaux acceptables, les normes doivent être totalement cohérentes avec les instruments de gouvernance des TI, étroitement alignées aux politiques de cybersécurité de l'entreprise et dictées par celles-ci.

Le diagramme ci-dessous illustre les éléments types d'une hiérarchie de gouvernance des TI. Les normes de cybersécurité sont l'interface essentielle entre les éléments de l'orientation et ceux de la mise en œuvre opérationnelle. Les normes sont indispensables pour orienter les objectifs et les résultats à atteindre au moyen des activités de mise en œuvre subséquentes, telles que l'élaboration des exigences fonctionnelles et techniques, l'architecture et la conception ainsi que les directives et procédures opérationnelles.

Figure 1 – Les normes de cybersécurité dans la hiérarchie de la gouvernance des TI



À toutes les étapes du processus de gouvernance des TI, une traçabilité directe est nécessaire pour assurer la conformité et garantir une gestion et une vérification efficaces. Les normes de cybersécurité doivent refléter les politiques de l'entreprise et ses obligations réglementaires externes (p. ex. normes et contrôles externes, tels que la réglementation financière ou en matière de confidentialité) et renvoyer à ces politiques et obligations.

Établir un cadre de gestion des normes

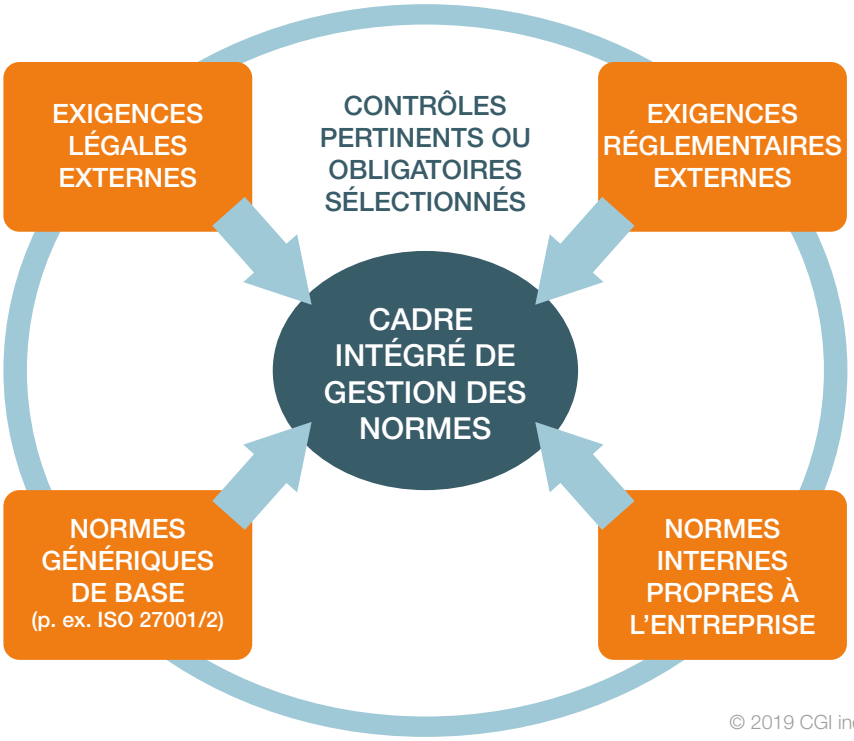
Pour la gestion des normes de cybersécurité, de nombreuses entreprises choisissent d'adopter un cadre générique, comme la famille de normes ISO/IEC 27001. Bien qu'ils constituent une excellente première étape, ces cadres de gestion n'abordent pas correctement toutes les obligations légales, réglementaires et commerciales de l'entreprise.

En effet, les normes génériques ne tiennent pas compte des exigences régionales ou sectorielles. Par exemple, une institution financière qui limite son cadre de gestion aux normes ISO/IEC 27001 s'expose à un risque et à une responsabilité potentielle en ne tenant pas compte des normes exigées par les organismes de réglementation pertinents, par exemple le Bureau du surintendant des institutions financières (BSIF), au Canada, ou d'autres exigences sectorielles ou régionales, comme celles imposées par le Conseil des normes de sécurité de l'industrie des cartes de paiement (PCI), par la Society for Worldwide Interbank Financial Telecommunication (SWIFT) ou par le Règlement général sur la protection des données (RGPD) de l'Union européenne.

L'entreprise devrait plutôt déterminer l'ensemble des exigences et des contrôles en matière de cybersécurité qu'elle doit respecter et les combiner à des normes sectorielles de base dans un cadre unique et intégré. Les raisons, à tout le moins générales, de l'inclusion de ces normes ou contrôles devraient figurer dans la stratégie et les politiques globales de cybersécurité de l'entreprise.

L'entreprise devrait déterminer l'ensemble des exigences et des contrôles en matière de cybersécurité qu'elle doit respecter et les inclure dans un cadre unique et intégré de gestion des normes de cybersécurité.

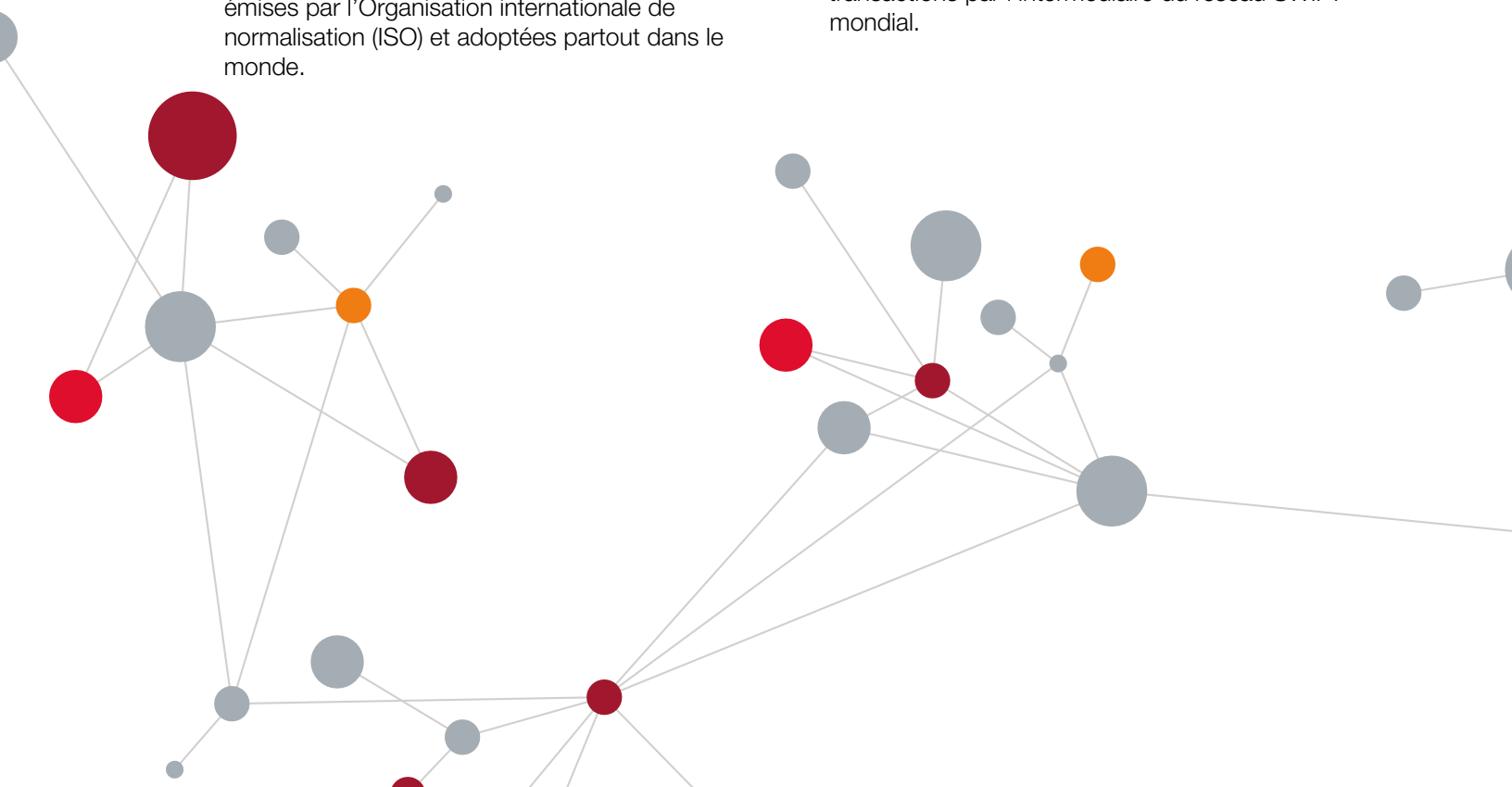
Figure 2 – Exemple de cadre intégré de gestion des normes de cybersécurité



NORMES EXTERNES

Les entreprises et les gouvernements sont tenus de se conformer à une série de normes, d'exigences et de mesures de contrôle externes en matière de cybersécurité et de confidentialité, et le non-respect de ces exigences peut avoir des conséquences punitives importantes. Voici quelques exemples :

- Cadre de gestion des risques NIST SP 800-53 (publication spéciale) ou ITSG-33. Ces cadres de gestion sont promulgués respectivement par le gouvernement fédéral des États-Unis et du Canada. Utilisés principalement par des organismes fédéraux, ces cadres ont également été adoptés par certaines entreprises du secteur. Ils fournissent une méthodologie ainsi qu'un catalogue de 900 contrôles détaillés et améliorations aux contrôles, à partir desquels un profil peut être créé pour répondre à presque toutes les exigences.
- Cadre de gestion de la cybersécurité NIST. Cette version plus « légère » du cadre de gestion NIST SP 800-53 est destinée à l'adoption par l'ensemble du secteur.
- ISO/IEC 27001. Ensemble de normes de sécurité émises par l'Organisation internationale de normalisation (ISO) et adoptées partout dans le monde.
- Bon nombre des objectifs de contrôle sont de nature générale, et les organisations doivent les compléter par des obligations externes en matière de conformité.
- RGPD. Réglementation obligatoire axée sur la confidentialité pour les entreprises qui traitent ou contrôlent des données personnelles appartenant à des citoyens de l'Union européenne. Les mesures punitives en cas de non-conformité ou de violation peuvent être sévères.
- Cyber Essentials. Imposé à l'origine aux entreprises faisant affaire avec le gouvernement du Royaume-Uni, cet ensemble de normes légères est maintenant adopté de façon plus générale comme solution de rechange au cadre de gestion de la cybersécurité NIST ou à la norme ISO 27001.
- PCI DSS. Cette norme de sécurité des données est obligatoire pour la plupart des entreprises qui recueillent, traitent et stockent les données des cartes de paiement (p. ex. Visa et MasterCard).
- Customer Security Control Framework (CSCF) de SWIFT. Ce cadre est requis pour les institutions financières participant au traitement des transactions par l'intermédiaire du réseau SWIFT mondial.



NORMES INTERNES

Chaque entreprise a des exigences précises pour se prémunir contre les risques propres à ses activités ou à son secteur d'activité. Souvent, ces exigences sont définies par la haute direction et intégrées dans la stratégie et les politiques de sécurité et de gestion des risques. Pour y répondre, l'entreprise doit se doter de normes et d'objectifs de contrôle personnalisés et les ajouter aux normes qu'elle a déjà adoptées (voir la figure 2 à la page 4).

La seule chose pire que l'absence de normes est l'adoption de normes imprécises, ambiguës ou impossibles à appliquer.

CRÉER DES NORMES INTERNES

Pour assurer la clarté et la pertinence des normes, l'entreprise doit respecter les 10 principes de base suivants :

1. **Liens avec les politiques.** En plus de s'harmoniser avec les besoins de l'entreprise, les normes doivent être liées aux politiques pour assurer une mise en œuvre uniforme. Si vos normes ne sont pas directement liées à la mise en œuvre d'une politique approuvée, attendez-vous à ce qu'elles soient contestées par ceux qui s'opposent à leur adoption.
2. **Collaboration.** Les normes de cybersécurité peuvent avoir des répercussions sur de nombreuses facettes de l'entreprise. Pour cette raison, il est essentiel de faire appel directement aux intervenants clés, comme les responsables des opérations TI et des catégories d'affaires, ainsi qu'aux services juridiques, de gestion des risques, de vérification et de confidentialité. Faites-en un sport d'équipe et acceptez les commentaires de tous les joueurs. Ainsi, ils auront l'impression d'avoir participé à l'élaboration des normes et seront moins susceptibles de s'opposer à leur adoption.
3. **Approbation par une autorité appropriée.** La mise en œuvre et le soutien des normes n'incombent pas uniquement à l'équipe de sécurité des TI. Par conséquent, il est essentiel que les normes soient « valorisées » et approuvées par une autorité centrale (p. ex. la haute direction). Autrement, elles risquent de ne pas être reconnues ni mises en œuvre dans l'ensemble de l'entreprise.
4. **Concision.** La longueur de la description d'une norme est inversement proportionnelle au nombre de personnes qui prendront le temps de la lire.
5. **Clarté.** Les normes imprécises donnent lieu à des mises en œuvre ambiguës, incohérentes et interprétatives. Les normes doivent indiquer clairement leur objectif dans des termes que tous les intervenants comprendront.
6. **Respect de l'intention.** Les normes doivent énoncer clairement l'état final souhaité et éviter de s'étendre sur la façon de le réaliser. La mise en œuvre d'une norme peut prendre différentes formes. Il vaut mieux laisser la décision aux personnes responsables de déployer la norme et de l'exécuter (dans la mesure où la norme donne le résultat voulu).
7. **Viabilité.** Il n'est pas judicieux de décrire une solution qui ne peut être réalisée sur le plan opérationnel ou technique. Pour assurer la viabilité des normes, les personnes responsables de leur élaboration doivent travailler de concert avec les autres intervenants (voir le paragraphe Collaboration).
8. **Vérifiabilité.** Pour que les normes soient efficaces, leur conformité doit faire l'objet d'un contrôle périodique. La nature humaine est telle que si le contrôle ou les examens de conformité d'une norme ne sont pas effectués, la norme sera peu à peu ignorée et son efficacité s'érodera rapidement. L'audit est un outil clé à cet égard (voir la section Mesurer la conformité des normes, à la page 10).
9. **Traçabilité.** L'établissement d'un lien direct entre les normes et les politiques de votre entreprise, ainsi qu'avec les normes externes, non seulement prouve l'importance de vos normes, mais facilite également leur mise à jour si les politiques et normes externes sont modifiées.
10. **Actualisation périodique.** Veillez à ce que vos normes de cybersécurité soient régulièrement revues et mises à jour. Les politiques, les technologies et les menaces évoluent. Les normes doivent aussi évoluer pour demeurer pertinentes, sinon elles seront considérées comme désuètes et seront ignorées.

COMPRENDRE LES NORMES DE CYBERSÉCURITÉ

Les normes de cybersécurité sont habituellement exprimées par écrit, surtout si elles comportent des exigences complexes. Lorsqu'ils sont présentés sous forme de document, au moins par catégorie (p. ex. normes de contrôle d'accès), les normes et les contrôles qui s'y rapportent peuvent être examinés par les intervenants concernés et approuvés par les autorités plus facilement.

Voici les exigences minimales relatives au contenu d'un document normatif type. N'oubliez pas que l'information relative à chaque élément doit être formulée de façon claire et concise :

- Numéro de catalogue ou de suivi de la norme.
- Date d'entrée en vigueur.
- Autorité approbatrice. Cette autorité doit être investie d'un pouvoir exécutif.
- Références clés. Cela comprend les politiques connexes.
- But. Il s'agit du but pour lequel la norme est créée.
- Objectifs. Il s'agit des résultats que la norme est censée permettre d'obtenir.
- Portée. Définition de ce qui est inclus dans le champ d'application de la norme et de ce qui en est exclu.
- Rôles et responsabilités. Affectations qui peuvent être exprimées sous forme de matrice RACI (responsabilité, approbation, consultation et information). Il est important de déterminer qui est responsable de l'ensemble de la norme et qui chapeaute chaque facette de sa mise en œuvre.
- Exigences. Cœur même de la norme. Les exigences doivent inclure une description claire de ce qu'il faut accomplir pour satisfaire à la norme. Elles peuvent comprendre plus d'un objectif et sont souvent appelées « objectifs de contrôle ». Les contraintes et les limites de la mise en œuvre doivent aussi y être décrites.
- Conformité et audit. Description de la façon dont la norme doit être surveillée et appliquée.
- Gestion des exceptions. Description du processus par lequel les exceptions à la norme doivent être approuvées et désignation des responsables.
- Liens de dépendance. Description des normes connexes dont dépend la norme de l'entreprise. Par exemple, une norme de contrôle d'accès peut dépendre d'une norme distincte d'authentification de l'utilisateur ou de gestion des privilèges.
- Contrôles externes connexes. Renvoi aux contrôles externes ou aux exigences réglementaires liées à la norme.
- Maintien de la norme. Description de la fréquence ou des périodes auxquelles la norme doit être revue et mise à jour et désignation des responsables. Un tableau des révisions doit également être fourni.

Les éléments suivants sont facultatifs, mais devraient être considérés pour faciliter la mise à l'essai et la vérification :

- Méthode d'essai et d'audit. Description de la façon dont l'efficacité de la norme (ou de ses objectifs de contrôle) doit être mise à l'essai ou dont la conformité à la norme doit être mesurée; il peut s'agir d'une brève description des interventions particulières d'essai ou d'audit qui démontreront la conformité (voir la section Mesurer la conformité des normes).

CRÉER UNE MATRICE DES NORMES

Les normes sont souvent résumées dans un tableau matriciel, comme une feuille de calcul, aussi appelé « profil de contrôle ». La création de cette matrice est importante, peu importe si les normes sont décrites sous une forme documentée. La matrice offre une vue globale des normes de l'entreprise et des contrôles qui s'y rapportent, ce qui facilite la gestion et permet de mieux comprendre les liens entre les normes. Elle est indispensable aux audits et aux essais de conformité.

Mesurer la conformité des normes

Il est nécessaire de mesurer la conformité et l'efficacité des normes pour atteindre les objectifs de manière durable. Autrement, les responsables de la mise en œuvre seront peu enclins à s'y conformer, et les risques visés par la norme ne seront pas atténués. La méthode ou le type de mesure choisi doit répondre aux objectifs opérationnels et aux exigences réglementaires.

« …mon accès aux [cibles majeures de l'entreprise] dépendait de la volonté des gens à contourner les politiques et procédures, qui étaient en place depuis des années avant que je réussisse à les déjouer. »

Kevin Mitnick, conseiller en sécurité informatique, auteur et pirate américain, mieux connu pour son arrestation hautement médiatisée en 1995 pour divers crimes liés à l'informatique et aux communications

CERTIFICATION

La certification est une attestation de conformité, généralement obtenue à la suite d'un audit externe. Elle confirme qu'une entreprise, un service ou un système se conforme à un ensemble de normes établi. La plupart des organismes de normalisation n'effectuent pas eux-mêmes les audits de certification. Les audits externes sont plutôt exécutés par des auditeurs indépendants qualifiés qui attestent le respect d'un ensemble précis de normes. Le rapport d'audit réussi et l'énoncé de conformité constituent la certification.

La certification peut également être effectuée en fonction de normes internes. Les grandes entreprises peuvent avoir un processus défini selon lequel les services ou systèmes – nouveaux ou considérablement modifiés – sont évalués avant de devenir opérationnels. Le but de cette évaluation est de déterminer si les politiques et les normes de sécurité de l'entreprise ont été respectées et, dans le cas contraire, quel est le risque résiduel pour l'entreprise. C'est ce qu'on appelle généralement le processus de « certification et accréditation ».

En plus d'être une carte de pointage utile pour la gestion des risques, la certification peut constituer un actif précieux pour l'entreprise, car elle lui permet de déclarer sa conformité aux normes de sécurité reconnues de l'industrie et, ainsi, d'assurer aux clients potentiels sa diligence et son intégrité en matière de sécurité.

MISES À L'ESSAI ET ÉVALUATIONS

Des essais sont souvent nécessaires pour assurer que les normes ont été mises en œuvre correctement et qu'elles sont conformes aux objectifs des normes ou aux contrôles en place. Par exemple, des systèmes de balayage pour détecter les mises à jour et correctifs de sécurité manquants seraient un moyen de vérifier la conformité à une norme de correction. Dans d'autres cas, la mise à l'essai peut comprendre l'élaboration et l'exécution de cas d'essai en fonction des objectifs de la norme ou de ses contrôles.

Les nouveaux systèmes et services doivent faire l'objet d'essais de conformité à toutes les normes pertinentes dès leur déploiement (ou avant, si un environnement de simulation réaliste peut être créé), puis périodiquement à des intervalles correspondant au cycle opérationnel de l'entreprise et selon sa situation en matière de risque et de sécurité. En raison de la nature changeante des systèmes de TI, des mises à l'essai annuelles sont recommandées.

AUDITS ET EXAMENS

Les mises à l'essai et les évaluations visent à déterminer le statut de conformité et l'efficacité d'une norme à un moment déterminé. Les audits et les examens permettent de déterminer si une norme et ses processus sont appliqués de façon uniforme sur une période donnée.

Les examens sont habituellement menés à l'interne et les résultats sont communiqués à la haute direction et aux autorités de gouvernance. Les audits, quant à eux, peuvent être effectués par des évaluateurs internes ou externes, mais dans tous les cas, les évaluateurs doivent être indépendants des responsables de la mise en œuvre quotidienne de la norme.

MESURER L'INCIDENCE DE LA NON-CONFORMITÉ

Les anomalies, lacunes et écarts relevés durant les mises à l'essai, les évaluations, les examens ou les audits doivent être évalués et considérés comme des risques pour l'entreprise. Les énoncés de risque doivent indiquer l'incidence potentielle sur la mission de l'entreprise, ses activités, ses services, ses actifs (y compris les systèmes et les données), sa réputation et sur la protection de la confidentialité.

En outre, les risques et leurs répercussions prévues doivent être classés par gravité, habituellement selon la stratégie et la politique de gestion des risques de l'entreprise et selon le degré de sensibilité des actifs. Les cotes de gravité les plus couramment utilisées sont les suivantes : FAIBLE, MOYENNE, ÉLEVÉE et CRITIQUE.

Responsabilité de la haute direction

La responsabilité de gérer les risques au sein de l'entreprise revient en dernier lieu à la haute direction. Celle-ci doit donc connaître les risques importants découlant des activités d'assurance de la conformité décrites ci-dessus. Une fois qu'elle dispose de toute l'information pertinente, la haute direction doit trancher : soit elle accepte les risques dans le cadre d'une décision opérationnelle éclairée, soit elle veille à ce que les ressources nécessaires à l'atténuation des risques soient disponibles.

Il n'est pas nécessaire d'informer la haute direction de chaque cas de non-conformité. Seuls les risques les plus graves doivent être portés à son attention, selon la stratégie et la politique de gestion des risques de l'entreprise. L'utilisation d'un registre des risques est le moyen habituel d'informer la haute direction.

UTILISER UN REGISTRE DES RISQUES

L'utilisation d'un registre des risques est de plus en plus courante pour informer tous les intervenants clés, y compris la haute direction, des risques graves qui pourraient avoir une incidence sur l'entreprise et pour suivre l'état et le traitement de ces risques jusqu'à leur acceptation ou leur atténuation. L'utilisation d'un registre des risques est donc une meilleure pratique courante en matière de gouvernance de la sécurité et de gestion des risques d'entreprise.

Le registre des risques est généralement mis à jour et présenté aux intervenants et à la haute direction à intervalles réguliers (p. ex. tous les trimestres), par l'intermédiaire d'un organe de gestion de la sécurité et des risques de haut niveau (p. ex. un comité directeur de la sécurité et des risques).

Le registre des risques est généralement présenté sous forme de tableau et comprend une description du risque, son incidence potentielle, les plans d'atténuation en place et la décision finale quant au traitement. Tous les risques ayant une incidence potentielle sur l'entreprise ou ses activités et jugés suffisamment graves pour nécessiter l'intervention des principaux décideurs font l'objet d'un suivi.

Par exemple, les risques de gravité ÉLEVÉE ou CRITIQUE, y compris ceux découlant de vulnérabilités de cybersécurité et de non-conformité aux normes, selon la tolérance au risque de l'entreprise, sa stratégie de gestion des risques et sa politique de catégorisation des risques.

La responsabilité de la gestion des risques au sein de l'organisation revient en dernier lieu à la haute direction. Pour s'en acquitter correctement, la haute direction doit être au courant des risques importants.

Conclusion

Tout bien pesé, les normes de cybersécurité constituent pour les entreprises un moyen crucial de s'assurer que leur stratégie et leurs politiques de sécurité font l'objet d'une mise en œuvre cohérente et mesurable dans le cadre des activités courantes.

Les normes peuvent être simples à adopter ou à créer. Cependant, elles doivent toutes exiger la participation d'une variété suffisante d'intervenants pour assurer leur viabilité et produire l'effet escompté sans nuire aux activités opérationnelles. Une fois adoptées, les normes doivent être mesurées régulièrement aux fins de mise en œuvre et de conformité, sinon leur efficacité s'érodera au fil du temps et les risques qu'elles visent ne seront pas atténués.

L'adoption de normes nécessite un investissement, mais celui-ci est minime par rapport aux conséquences potentielles d'un incident majeur de cybersécurité. De plus, cet investissement augmentera la confiance et l'assurance de tous les intervenants, y compris la haute direction, les conseils d'administration, les organismes de réglementation, les actionnaires, les clients et le public.

CGI

À propos de CGI

Fondée en 1976, CGI est l'une des plus importantes entreprises de services-conseils en technologie de l'information (TI) et en management au monde. Exerçant ses activités partout dans le monde, CGI offre des capacités complètes notamment des services-conseils en TI et en management, des services d'intégration de systèmes et d'impartition ainsi que des solutions de propriété intellectuelle. Celles-ci aident nos clients à atteindre leurs objectifs, y compris devenir des organisations numériques axées sur le client.

Les capacités de CGI en matière de cybersécurité sont vastes et approfondies. Elles nous permettent d'offrir à nos clients gouvernementaux et commerciaux une expertise de calibre mondial dans les domaines de la gestion déléguée des services de sécurité, des services-conseils en cybersécurité et de l'évaluation. Les entreprises font appel à CGI pour évaluer les risques, créer une infrastructure et des systèmes sécurisés, et exploiter leurs activités en toute confiance. La cybersécurité est centrale à notre approche : les contrôles sont intégrés, et non ajoutés après coup.

Forte d'une expertise et d'une expérience unique, CGI aide ses clients à concevoir des mesures efficaces de gouvernance de cybersécurité et de gestion des risques afin de contrer les menaces dans un monde numérique de plus en plus connecté.

Communiquez avec nous pour savoir comment nous pouvons vous aider :

Tél : +1-613-234-2155
Courriel : GlobalCyberSecurity@cgi.com