Diligent

SRI 2 : Êtes-vous prêt à relever la barre de la GRC dans le domaine de la cybersécurité ?

Se préparer à la mise en conformité avec la SRI 2

Dans notre univers numérique hyperconnecté, les réseaux technologiques accompagnent les sociétés et les économies. La Covid-19 a accéléré notre dépendance numérique en remplaçant les interactions personnelles par des processus en ligne, ce qui nous a aidés à surmonter de nombreux défis liés à la pandémie.

Mais si la numérisation nous a permis de faire un bond en avant en termes de rapidité et de commodité, elle a également introduit des risques. Lorsque nos réseaux d'énergie, d'approvisionnement en eau, nos services de santé, nos établissements bancaires, nos réseaux de transport, etc., dépendent d'une infrastructure numérique, celle-ci doit être robuste, fiable et protégée contre les perturbations causées par des cyberattaques.

Dans un environnement géopolitique et socioculturel instable, de telles attaques, qu'elles soient le fait d'acteurs parrainés par l'État-nation ou d'entreprises criminelles, sont inévitables et peuvent mettre des vies en danger. De plus, l'interconnexion des réseaux signifie qu'une attaque contre une entreprise, dans un pays, peut rapidement s'intensifier et toucher un grand nombre d'organisations dans plusieurs pays. Il n'est pas facile de fermer les frontières à une cyberattaque.

Reconnaissant ce risque croissant, l'Union européenne a introduit la première directive sur les réseaux et les systèmes d'information en 2016. Son objectif était d'améliorer la résilience des réseaux et des systèmes d'information de l'Union face aux risques de cybersécurité et de prévenir les attaques susceptibles de perturber le bien-être physique, social et économique de ses citoyens. Pour lui succéder, la directive SRI 2 est actuellement en cours de transposition dans la législation des États membres de l'UE. À partir d'octobre 2024, elle s'appliquera à toutes les entités désignées comme « essentielles » et « importantes » dans un large éventail de secteurs critiques pour le bon fonctionnement de la société moderne.

Le champ d'application de la SRI 2 est plus vaste et inclut de nouveaux domaines d'activités et de responsabilités. Les sanctions en cas de non-conformité sont lourdes et reflètent la gravité potentielle des perturbations des infrastructures nationales (et internationales) critiques. La directive cible également la cybersécurité de la chaîne d'approvisionnement, ce qui produira un effet boule de neige au-delà des organisations directement tenues de s'y conformer.

La SRI 2 met en place le principe de responsabilité en matière de gouvernance, de gestion des risques et de conformité, non seulement pour les entités « essentielles » et « importantes », mais aussi pour les milliers d'entreprises chargées de fournir ces entités. Des compétences en matière de leadership à l'établissement d'une culture de la sécurité, en passant par les contrôles internes et le suivi, nombreux sont les facteurs multidisciplinaires à prendre en compte.

Dans ce livre blanc, nous allons examiner la SRI 2, ses exigences et les points sur lesquels les entreprises devraient concentrer leurs travaux préparatoires.

Table des matières

En quoi consiste la directive sur les réseaux et les systèmes d'information ?

La directive SRI a été mise en œuvre en 2016. Il s'agissait de la première tentative de l'Union européenne de créer un niveau homogène de compétence en matière de cybersécurité au sein des organisations qui fournissent des infrastructures et des services critiques aux citoyens de l'UE. Son objectif était de protéger ces derniers contre l'impact des cyberattaques.

La directive a connu un certain succès, mais elle avait ses limites. Sa mise en œuvre n'était pas uniforme entre les zones géographiques et il n'existait aucun dispositif permettant de répondre conjointement aux crises. Dans le même temps, l'accélération rapide de la numérisation provoquée par la pandémie a accru la dépendance numérique et augmenté la quantité de cibles que les acteurs malveillants cherchent à attaquer.

Depuis 2016, de nouvelles technologies sont apparues, notamment des outils d'intelligence artificielle accessibles à tous. Avec elles sont apparus de nouveaux vecteurs de menaces et le renforcement des compétences, dans une plus grande cohorte de cybercriminels. Les risques de cybersécurité ont augmenté en conséquence. La combinaison de tous ces défis a incité l'UE à concevoir et à mettre en œuvre la directive SRI 2.

Quoi de nouveau dans la SRI 2 ?

- **Un champ d'application plus étendu** : quinze secteurs d'activité sont désormais inclus dans le champ d'application de la directive. Les nouvelles règles garantissent l'inclusion de toutes les moyennes et grandes entreprises.
- **La responsabilité personnelle** : les équipes de direction sont tenues de superviser et d'approuver les mesures de cybersécurité de l'entité.
- **La révision du dispositif minimum de sécurité** : les entités sont tenues d'adopter une approche de la gestion des risques en appliquant une liste d'éléments de sécurité de base a minima.
- **Des exigences de reporting plus prescriptives** : des processus plus précis pour le signalement des incidents ont été mis en place, avec des délais plus courts et des exigences de contenu pour les notifications des violations.
- **La gestion de la chaîne d'approvisionnement** : les entreprises doivent traiter les risques de cybersécurité dans leur chaîne d'approvisionnement. Les organisations de niveau européen telles que l'ENISA (Agence de l'Union européenne pour la cybersécurité) sont également autorisées à effectuer des évaluations des risques et des évaluations des chaînes d'approvisionnement transfrontalières critiques.
- **La collaboration et la coopération** : la directive SRI 2 impose la création d'équipes spécialisées dans la gestion des incidents de sécurité informatique (CSIRT) dans chaque État membre et les oblige à collaborer avec leurs homologues des autres pays. Un cadre pour la divulgation coordonnée des vulnérabilités, la création d'une base de données européenne sur les vulnérabilités et des travaux préparatoires pour une réponse conjointe aux crises sont également inclus.

Quelle est la date limite de mise en conformité ?

Les États membres de l'UE doivent transposer la directive dans leur législation locale d'ici le 17 octobre 2024. Certains États de l'UE sont légèrement en retard sur le calendrier[1], mais les entreprises assujetties à la SRI 2 et leurs fournisseurs ne devraient pas ajourner les travaux préparatoires de mise en conformité.

[1] https://www.osborneclarke.com/insights/what-eu-businesses-need-know-about-nis2-and-cybersecurity-compliance#:~:text=The%2021%2Dmonth%20implementation%20period,directive%20into%20their%20national%20laws.

Secteurs critiques soumis à la SRI 2

Secteurs à haute criticité :

- **Énergie**
- **Transports**
- **Services bancaires**
- **Santé** (y compris les fabricants de vaccins et d'appareils médicaux)
- **Eau** (eau potable et eaux usées)
- **Fournisseurs d'infrastructures numériques** (y compris les fournisseurs de services gérés)
- **Aérospatiale**
- **Administration publique**

Autres secteurs critiques :

- **Services postaux**
- **Gestion des déchets**
- **Alimentation**
- **Produits chimiques**
- **Entreprises manufacturières** (divers secteurs, notamment les dispositifs médicaux, les ordinateurs et l'électronique, les machines et les équipements)
- **Fournisseurs numériques** (notamment les places de marché en ligne, les moteurs de recherche, les plateformes de réseaux sociaux)
- **Organismes de recherche**

En matière de cybersécurité, chaque secteur d'activité est confronté à des défis spécifiques qui peuvent être liés à différents facteurs : le niveau de numérisation, la mesure dans laquelle il s'appuie sur un patrimoine numérique hérité ou sur des processus obsolètes, le niveau d'informations personnelles identifiables sur les citoyens qu'il gère et les ressources dont il dispose.

Lorsqu'elles ciblent la conformité à la SRI 2, les organisations doivent tenir compte des risques spécifiques à leur secteur et les aborder à la lumière des dispositions de la directive.

Que sont les entités « essentielles » et les entités « importantes » ?

La SRI 2 classe les entreprises concernées comme étant « essentielles » ou « importantes ».

Les critères de qualification pour chaque catégorie varient légèrement d'un secteur à l'autre, mais en voici un aperçu :

- **Les entités essentielles** fournissent des produits et/ou des services dans l'un des secteurs spécifiés et comptent plus de 250 employés, un chiffre d'affaires annuel de 50 millions d'euros ou plus ou un bilan de 43 millions d'euros ou plus.
- **Les entités importantes** fournissent des produits et/ou des services dans l'un des secteurs spécifiés et comptent plus de 50 employés, un chiffre d'affaires annuel de 10 millions d'euros ou plus ou un bilan de 10 millions d'euros ou plus.

Impact sur la chaîne d'approvisionnement

La directive SRI 2 aura un impact bien au-delà des entités directement concernées. Elle oblige les entités essentielles et importantes à mettre en place un dispositif minimum de sécurité tout au long de la chaîne d'approvisionnement pour leurs produits et services. Leurs fournisseurs seront soumis à une surveillance accrue et tenus de respecter des normes de cybersécurité plus strictes que celles qu'ils appliquaient auparavant.

De plus, bien que les entreprises britanniques ne soient pas directement touchées par la SRI 2, celles qui approvisionnent des entités européennes essentielles ou importantes devront prouver à leurs clients qu'elles opèrent selon les normes de la directive.

Au total, on estime que plus de 160 000 entreprises seront concernées par la SRI 2.

Dans l'ensemble, l'inclusion des entreprises de la chaîne d'approvisionnement créera un effet de marée montante, renforçant ainsi la résilience de l'ensemble de l'écosystème numérique. C'est un résultat souhaitable, mais qui signifie qu'un grand nombre d'organisations doivent renforcer la gouvernance, la gestion des risques et la conformité en matière de cybersécurité.

Quelles sont les sanctions en cas de manquement aux dispositions de la SRI 2 ?

Les sanctions en cas de manquement aux obligations de gestion des risques et de reporting de la SRI 2 sont lourdes, reflétant ainsi le potentiel perturbateur des failles de cybersécurité. Il s'agit notamment de :

Sanctions non financières

- Instructions contraignantes qui doivent être suivies
- Mise en œuvre obligatoire des recommandations des audits de sécurité
- Injonctions visant à aligner les mesures de sécurité sur les exigences de la SRI 2
- Alertes obligatoires à communiquer aux clients des entités à propos des risques

Sanctions financières

- **Entités essentielles :** une amende d'au moins 10 millions d'euros ou de 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, selon le montant le plus élevé.
- **Entités importantes :** une amende d'au moins 7 millions d'euros ou de 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, selon le montant le plus élevé.

Sanctions en matière de gestion

La directive SRI 2 prend acte du rôle essentiel de la haute direction dans la supervision de la cybersécurité, l'assurance de cybersécurité et la sensibilisation à cette question au sein des organisations. Elle vise à alléger les responsabilités des services informatiques en matière de sécurité et à garantir que les aspects de cybersécurité sont correctement classés et gérés en tant que risques organisationnels stratégiques.

La SRI 2 tient les dirigeants pour directement responsables des négligences identifiées en cas de violations. Les sanctions incluent :

- la divulgation publique obligatoire des manquements à la conformité ;
- la publication des personnes et entités impliquées dans la violation, ainsi que d'informations spécifiques concernant l'incident ;
- les dirigeants d'entités essentielles impliquées dans des manquements à la conformité peuvent se voir temporairement interdire d'occuper des postes de direction si les manquements persistent ou se reproduisent.

Par conséquent, la SRI 2 représente un renforcement considérable de la responsabilité qui incombe aux dirigeants, dans le but de garantir que la cybersécurité reçoit le niveau d'attention approprié du point de vue de la gouvernance, de la gestion des risques et de la conformité.

Principales implications de la SRI 2 sur la GRC

En tant que directive basée sur la gestion des risques qui fait également porter la responsabilité de la conformité à la haute direction, la SRI 2 exigera des activités de GRC à la fois stratégiques et tactiques. Les articles 20, 21 et 23 de la directive contiennent de nombreux détails concernant ce que l'on attend des entités essentielles et importantes en termes de gouvernance, de gestion des risques et de reporting, dans le domaine de la cybersécurité.

Gouvernance

Les organes de direction des entités essentielles et importantes doivent approuver les mesures de gestion des risques de cybersécurité mises en place au sein de l'organisation, et ces organes peuvent être tenus responsables en cas d'infraction.

Par conséquent, les organes de direction auront besoin d'obtenir de l'entreprise la garantie que celle-ci a adopté des mesures et des politiques en ce sens, et qu'elles sont appliquées efficacement.

Ils sont également tenus de suivre une formation en cybersécurité afin de s'assurer qu'ils possèdent « les connaissances et les compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité ».[2]

Les conseils d'administration doivent s'interroger sur l'expérience et les compétences en cybersécurité de leurs membres. Si l'expérience n'est pas disponible, ils devraient donner la priorité aux compétences dans ce domaine lors des nouvelles nominations.

Article 21 : mesures a minima de gestion des risques de cybersécurité pour la protection des réseaux et des systèmes d'information :

a. les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information ;
b. la gestion des incidents ;
c. la continuité des activités, par exemple la gestion des sauvegardes et de la reprise des activités, et la gestion des crises ;
d. la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs ;
e. la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités ;
f. les politiques et procédures visant à évaluer l'efficacité des mesures de gestion des risques de cybersécurité ;
g. les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité ;
h. des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;
i. la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs ;
j. l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence sécurisés au sein de l'entité, selon les besoins.

Source : https://eur-lex.europa.eu/eli/dir/2022/2555, article 21, paragraphe 2

[2] https://eur-lex.europa.eu/eli/dir/2022/2555 Article 21

Risque

Les organisations sont tenues de mettre en œuvre des mesures garantissant un niveau de cybersécurité proportionné et adapté aux risques posés, ce qui implique d'appliquer les principes de gestion des risques à l'ensemble de l'environnement des réseaux et des systèmes d'information.

Comme indiqué précédemment, cet environnement inclut également les fournisseurs. Les entités essentielles et importantes doivent avoir de la visibilité sur les performances de cybersécurité de leurs principaux fournisseurs. Elles doivent évaluer la qualité des produits et les pratiques de cybersécurité des fournisseurs, et la directive mentionne spécifiquement la vérification des pratiques de développement de logiciels sécurisés. Cela reflète la récente recrudescence des attaques contre la chaîne d'approvisionnement logicielle, comme l'attaque de Solarwinds, qui a démontré la vulnérabilité des logiciels utilisant des composants de tiers.

Le dynamisme de l'environnement des cybermenaces signifie que la surveillance continue des fournisseurs est également essentielle, afin de permettre aux organisations de suivre leur exposition aux risques et de réagir lorsque de nouvelles menaces apparaissent.

Les mesures de continuité des activités constituent une autre exigence explicite. Les organisations doivent s'assurer d'avoir mis en œuvre de solides mesures de continuité des activités, afin de minimiser l'impact des violations. Ces mesures doivent être basées sur une compréhension claire des cybermenaces, de leur probabilité et de leur impact potentiel sur l'organisation et ses clients.

Conformité

Pour garantir la conformité aux dispositions de la SRI 2, des contrôles efficaces de la gestion et de la surveillance de la cybersécurité, interne et des tiers, doivent être mis en œuvre.

L'organisation doit également concevoir et mettre en place plusieurs politiques, en particulier des politiques en matière d'analyse des risques et de sécurité de l'information, des politiques visant à évaluer l'efficacité des mesures de gestion des risques de cybersécurité et des politiques concernant des domaines technologiques spécifiques tels que le chiffrement et les contrôles d'accès.

L'entreprise doit s'assurer que des procédures sont en place pour signaler toute violation dans les délais et avec les détails requis. Dans le cadre de la préparation à la gestion de crise, il est conseillé de réaliser des exercices d'entraînement simulant une violation majeure et testant les cadres mis en place, afin de réagir efficacement aux incidents.

SRI 2 : calendrier de signalement des incidents

Survenance d'un incident important ou d'une cybermenace

Dans les 24 heures : envoi d'une première notification aux autorités compétentes ou à l'équipe CSIRT, en indiquant si l'incident est présumé être dû à une action illégale ou malveillante.

À la demande de l'autorité compétente ou de l'équipe CSIRT : rédaction d'un rapport intermédiaire fournissant des mises à jour pertinentes.

Dans le mois suivant la première notification : remise d'un rapport final, comprenant au minimum une description détaillée de l'incident, de sa gravité et de son impact, le type de menace ou la cause première qui l'a probablement déclenché, une description des mesures d'atténuation appliquées et des activités en cours pour y remédier.

Maintenant, sur quoi axer la GRC ?

Si votre organisation entre maintenant dans le champ d'application de la SRI 2, ou si vous êtes l'un des fournisseurs clés d'une organisation qui y est assujettie, vous devez agir rapidement pour définir le travail nécessaire à la mise en conformité. Si vous étiez déjà soumis à la SRI, concentrez-vous sur le respect des dispositions supplémentaires de la SRI 2.

Voici quelques-unes des principales actions que les professionnels de la GRC devraient engager :

Gouvernance

- [ ] Veillez à ce que la SRI 2 reçoive du conseil d'administration et de la direction l'attention qui lui est due.
- [ ] Révisez la composition du conseil d'administration en fonction des compétences et de l'expérience en matière de cybersécurité.
- [ ] Mettez en place une formation à la cybersécurité pour le conseil d'administration et l'équipe de direction. Veillez à ce qu'une formation appropriée de sensibilisation à la cybersécurité soit mise en place pour l'ensemble de l'organisation.

Risque

- [ ] Évaluez votre situation en matière de cybersécurité et analysez vos lacunes par rapport aux exigences de la SRI 2.
- [ ] Déterminez votre niveau de visibilité sur la cybersécurité de la chaîne d'approvisionnement et mettez en œuvre un programme de gestion des risques de tiers ou renforcez le vôtre.
- [ ] Assurez-vous que les risques de cybersécurité spécifiques à votre secteur sont identifiés et gérés.

Conformité

- [ ] Créez un environnement de contrôle couvrant les domaines pertinents de la SRI 2 afin d'offrir l'assurance requise aux organes de direction.
- [ ] Assurez-vous que des politiques sont en place concernant l'analyse des risques et la sécurité de l'information, l'efficacité de la gestion des risques et les domaines spécifiques à la technologie.
- [ ] Concevez et testez des plans de réponse aux incidents. Identifiez le personnel interne et externe clé, y compris au sein des principaux fournisseurs, à inclure dans les plans de réponse aux incidents et effectuez des exercices pratiques.
- [ ] Identifiez les interdépendances et les domaines couverts par d'autres réglementations ou normes, telles que le NIST, le RGPD, la norme ISO 27001 et la PCI-DSS, dans lesquels une gestion des risques et des politiques sont déjà en place. Vous éviterez ainsi de refaire un travail qui a déjà été réalisé.

Communications

- [ ] Informez vos fournisseurs clés qu'avec l'entrée en vigueur de la SRI 2, vous allez mettre en œuvre une évaluation et une surveillance de la cybersécurité. Créez un cadre de collaboration avec eux afin de résoudre les problèmes identifiés.
- [ ] Confirmez que l'organisation dispose de canaux de communication d'urgence sécurisés et résilients qui resteront opérationnels en cas de violation (conformément à l'article 21, paragraphe 2, point j de la directive).

Obtenez de la visibilité sur la conformité à la directive SRI 2 grâce à Diligent One.

La SRI 2 est une directive de grande envergure qui nécessite une réponse à plusieurs niveaux et dans plusieurs disciplines. Cela implique de gérer les risques d'entreprise, les risques informatiques et les risques de tiers, en intégrant des contrôles visant à garantir l'efficacité des programmes.

Les organisations ne doivent pas traiter la conformité à la directive SRI 2 de manière isolée, mais au contraire s'assurer que la visibilité et la transparence sont présentes à tous les niveaux, dès le conseil d'administration, par le biais des principaux services informatiques, juridiques, de RH et financiers. Une plateforme GRC complète comme Diligent One permet aux organisations d'aborder la SRI 2 de manière globale, d'éviter les doublons et de garantir que les informations de reporting requises sont facilement accessibles à toutes les parties prenantes lorsqu'elles en ont besoin.

Diligent

À propos de Diligent

Diligent est la société SaaS leader dans le domaine de la gouvernance, des risques et de la conformité (GRC). Un million d'utilisateurs chez plus de 25 000 clients dans le monde font appel à ses services. Notre technologie innovante offre aux dirigeants une vision connectée de la gouvernance, des risques, de la conformité et des critères ESG au sein de leurs organisations. Elle leur fournit les informations dont ils ont besoin pour prendre de meilleures décisions et diriger avec détermination. Pour en savoir plus, consultez diligent.com/fr.

Pour obtenir davantage d'informations ou demander une démonstration :

info@diligent.com | diligent.com/fr

1289572732