COMMISSION
EUROPÉENNE

Bruxelles, le 3.2.2025
C(2025) 618 final

ANNEXES 1 to 2

ANNEXES

de la

Décision d'exécution de la Commission

relative à une demande de normalisation adressée au Comité européen de normalisation (CEN), au Comité européen de normalisation électrotechnique (Cenelec) et à l'Institut européen de normalisation des télécommunications (ETSI) portant sur les produits comportant des éléments numériques, à l'appui du règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience)

ANNEXE I

Liste des nouvelles normes européennes à élaborer

Informations de référence		Délai d'adoption par les OEN
Normes horizontales concernant des exigences de sécurité relatives aux propriétés des produits comportant des éléments numériques		
1.	Norme(s) européenne(s) sur la conception, le développement et la fabrication de produits comportant des éléments numériques de manière à garantir un niveau approprié de cybersécurité en fonction des risques	30 août 2026
2.	Norme(s) européenne(s) relative(s) à la mise à disposition sur le marché de produits comportant des éléments numériques sans vulnérabilités exploitables connues	30 octobre 2027
3.	Norme(s) européenne(s) relative(s) à la mise à disposition sur le marché de produits comportant des éléments numériques avec une configuration sécurisée par défaut	30 octobre 2027
4.	Norme(s) européenne(s) visant à faire en sorte que les vulnérabilités des produits comportant des éléments numériques puissent être traitées au moyen de mises à jour de sécurité	30 octobre 2027
5.	Norme(s) européenne(s) visant à assurer la protection des produits comportant des éléments numériques contre tout accès non autorisé et à signaler un éventuel accès non autorisé	30 octobre 2027
6.	Norme(s) européenne(s) sur la protection de la confidentialité des données stockées, transmises ou traitées d'une autre manière par un produit comportant des éléments numériques	30 octobre 2027
7.	Norme(s) européenne(s) sur la protection de l'intégrité des données, commandes, programmes d'un produit comportant des éléments numériques et sa configuration	30 octobre 2027

	contre toute manipulation ou modification non autorisée par l'utilisateur, ainsi que la communication d'informations sur les corruptions	
8.	Norme(s) européenne(s) relative(s) au traitement des données, à caractère personnel ou autres, limité à celles qui sont adéquates, pertinentes et à ce qui est nécessaire par rapport à l'utilisation prévue du produit («minimisation des données»);	30 octobre 2027
9.	Norme(s) européenne(s) sur la protection de la disponibilité des fonctions élémentaires et essentielles du produit comportant des éléments numériques	30 octobre 2027
10.	Norme(s) européenne(s) visant à réduire au minimum l'incidence négative d'un produit comportant des éléments numériques ou de ses dispositifs connectés sur la disponibilité des services fournis par d'autres dispositifs ou réseaux	30 octobre 2027
11.	Norme(s) européenne(s) relative(s) à la conception, au développement et à la fabrication de produits comportant des éléments numériques avec des surfaces d'attaque limitées	30 octobre 2027
12.	Norme(s) européenne(s) sur la conception, le développement et la fabrication de produits comportant des éléments numériques qui réduisent l'impact d'un incident à l'aide de mécanismes et de techniques appropriés de limitation de l'exploitation de failles;	30 octobre 2027
13.	Norme(s) européenne(s) sur la fourniture d'informations relatives à la sécurité par l'enregistrement et/ou le suivi de l'activité interne pertinente des produits comportant des éléments numériques, tout en laissant à l'utilisateur la possibilité de désactiver le mécanisme	30 octobre 2027
14.	Norme(s) européenne(s) sur la suppression ou le transfert, en toute sécurité et facilement, de l'ensemble des données et paramètres d'un produit comportant des	30 octobre 2027

	éléments numériques.	
Normes horizontales relatives aux exigences en matière de traitement des vulnérabilités		
15.	Norme(s) européenne(s) sur la gestion des vulnérabilités pour les produits comportant des éléments numériques	30 août 2026
Normes verticales concernant des exigences de sécurité relatives aux propriétés des produits comportant des éléments numériques		
16.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les systèmes de gestion de l'identité et les logiciels et matériels de gestion des accès privilégiés, notamment les lecteurs pour l'authentification et le contrôle d'accès, y compris les lecteurs biométriques	30 octobre 2026
17.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les navigateurs autonomes et intégrés	30 octobre 2026
18.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les gestionnaires de mots de passe	30 octobre 2026
19.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les logiciels qui recherchent, suppriment ou mettent en quarantaine des logiciels malveillants	30 octobre 2026
20.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les produits comportant des éléments numériques ayant la fonction de réseau privé virtuel (VPN)	30 octobre 2026
21.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les systèmes de gestion de réseau	30 octobre 2026
22.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les systèmes de gestion des informations et des événements en matière de sécurité (SIEM)	30 octobre 2026
23.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité	30 octobre 2026

	pour les gestionnaires de démarrage	
24.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les infrastructures à clés publiques et les logiciels de délivrance de certificats numériques	30 octobre 2026
25.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les interfaces réseau physiques et virtuelles	30 octobre 2026
26.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les systèmes d'exploitation	30 octobre 2026
27.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les routeurs, les modems destinés à la connexion à l'internet et les commutateurs	30 octobre 2026
28.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les microprocesseurs dotés de fonctionnalités liées à la sécurité;	30 octobre 2026
29.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les microcontrôleurs dotés de fonctionnalités liées à la sécurité;	30 octobre 2026
30.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les circuits intégrés spécifiques à une application (ASIC) et les réseaux de portes programmables sur le terrain (FPGA) avec des fonctionnalités liées à la sécurité	30 octobre 2026
31.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les assistants virtuels polyvalents pour maison intelligente	30 octobre 2026
32.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les produits domestiques intelligents dotés de fonctionnalités de sécurité, y compris les serrures de porte intelligentes, les caméras de sécurité, les systèmes de surveillance pour bébés et les systèmes	30 octobre 2026

	d’alarme	
33.	Norme(s) européenne(s) relative(s) aux exigences essentielles en matière de cybersécurité applicables aux jouets connectés à l’internet couverts par la directive 2009/48/CE, dotés de caractéristiques sociales interactives (par exemple, parler ou filmer) ou de fonctions de suivi de localisation	30 octobre 2026
34.	Norme(s) européenne(s) relative (s) aux exigences essentielles en matière de cybersécurité applicables aux produits portables personnels à porter ou à placer sur un corps humain à des fins de surveillance de la santé (comme le suivi) et auxquels le règlement (UE) 2017/745 ou le règlement (UE) 2017/746 ne s’appliquent pas, ou aux produits portables personnels destinés à être utilisés par et pour les enfants	30 octobre 2026
35.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les hyperviseurs et systèmes d’exécution de conteneurs prenant en charge l’exécution virtualisée de systèmes d’exploitation et d’environnements similaires	30 octobre 2026
36.	Norme(s) européenne(s) relative(s) aux exigences essentielles en matière de cybersécurité pour les pare-feu, les systèmes de détection et/ou de prévention des intrusions, y compris ceux spécifiquement destinés à un usage industriel	30 octobre 2026
37.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les microprocesseurs inviolables	30 octobre 2026
38.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les microcontrôleurs inviolables;	30 octobre 2026
39.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les dispositifs matériels avec boîtiers	30 octobre 2026

	de sécurité;	
40.	Norme(s) européenne(s) relative(s) aux exigences essentielles en matière de cybersécurité concernant les passerelles pour compteurs intelligents au sein des systèmes intelligents de mesure tels que définis à l'article 2, point 23), de la directive (UE) 2019/944 et d'autres dispositifs à des fins de sécurité avancées, y compris pour le cryptotraitement sécurisé	30 octobre 2026
41.	Norme(s) européenne(s) sur les exigences essentielles en matière de cybersécurité pour les cartes à puce ou dispositifs similaires, y compris les éléments sécurisés	30 octobre 2026

ANNEXE II

Exigences relatives aux nouvelles normes européennes visées à l'article 1er

1. Exigences applicables aux normes européennes demandées

Objectifs

Les normes européennes harmonisées reflètent l'état de la technique généralement reconnu[1] afin de réduire au minimum les risques en matière de cybersécurité qui surviennent lors de la planification, de la conception, du développement, de la fabrication, de la livraison et de la maintenance de produits comportant des éléments numériques, afin de prévenir les incidents de sécurité et de réduire au minimum les conséquences de ces incidents, y compris en ce qui concerne la santé et la sécurité des utilisateurs.

Les normes européennes harmonisées fournissent, dans la mesure nécessaire et en tenant compte de l'état de la technique, des spécifications techniques fondées sur la technologie, le processus ou la méthodologie en ce qui concerne la conception et le développement de produits comportant des éléments numériques, y compris des procédures d'évaluation telles que des essais et des examens, avec des critères objectivement vérifiables et des méthodes applicables pour évaluer le respect de ces spécifications.

Des spécifications d'appui ou d'autres éléments livrables de normalisation (par exemple, en ce qui concerne la terminologie[2]) sont définies et fournies lorsque cela est nécessaire pour garantir la cohérence et la mise en œuvre des normes européennes. Ces spécifications peuvent également comprendre des éléments utiles pour les normes horizontales et verticales, tels que des catalogues des contrôles de sécurité, des menaces, des vulnérabilités, des méthodes d'attaque, des spécifications relatives à la communication et des instructions aux utilisateurs, ainsi que des dispositions relatives à l'accessibilité.

Cohérence

Les normes harmonisées élaborées en réponse à la présente demande devraient s'appuyer sur les travaux en cours d'élaboration afin de soutenir l'application du règlement délégué (UE) 2022/30 de la Commission[3], sans préjudice des améliorations nécessaires. Les spécificités du règlement (UE) 2024/2847[4] doivent toutefois être pleinement prises en compte au cours de la phase de développement. Dans la mesure du possible, le CEN, le Cenelec et l'ETSI peuvent

---

[1] L'état de la technique n'implique pas nécessairement les recherches scientifiques les plus récentes encore à un stade expérimental ou dont la maturité technologique est insuffisante. L'état de la technique ne doit pas être conçu comme représentant des exigences minimales pour accéder au marché.

[2] Toutes les normes européennes élaborées sur la base de la présente demande reposent sur une terminologie commune. Les spécifications d'appui relatives à la terminologie doivent en outre se fonder autant que possible sur la terminologie adoptée au niveau international et notamment dans les normes internationales.

[3] Règlement délégué (UE) 2022/30 de la Commission du 29 octobre 2021 complétant la directive 2014/53/UE du Parlement européen et du Conseil en ce qui concerne l'application des exigences essentielles visées à l'article 3, paragraphe 3, points d), e) et f), de cette directive (JO L 7 du 12.1.2022, p. 6, ELI: http://data.europa.eu/eli/reg_del/2022/30/oj).

[4] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847 du 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

mettre à jour les normes et publications en matière de normalisation existantes afin de les aligner sur les exigences du règlement sur la cyberrésilience.

Sans préjudice des améliorations nécessaires, le CEN, le Cenelec et l'ETSI veillent à ce que les normes européennes produites soient cohérentes, le cas échéant, avec d'autres normes européennes et harmonisées élaborées ou en cours d'élaboration dans les différents secteurs concernés, notamment celles liées aux produits couverts par la législation de l'UE, tels que la directive 2006/42/CE du Parlement européen et du Conseil[5], les règlements (UE) 2023/1230[6], (UE) 2024/1689[7], (UE) 2023/1781[8] ou les schémas de certification de cybersécurité de l'UE élaborés ou en cours d'élaboration au titre du règlement (UE) 2019/881 du Parlement européen et du Conseil[9]. En outre, le CEN, le Cenelec et l'ETSI devraient veiller à ce que les normes harmonisées élaborées en réponse à la présente décision soient compatibles avec les obligations de l'Union découlant des accords et traités internationaux.

Champ d'application des normes européennes

Chaque norme européenne harmonisée indique clairement son champ d'application, les produits qui relèvent de son champ d'application, les risques couverts et les autres risques pertinents qui ne sont pas couverts. Lorsqu'une norme harmonisée ne couvre pas toutes les exigences essentielles qui sont applicables aux produits relevant de son champ d'application, elle indique les exigences essentielles qui ne sont pas entièrement couvertes. Lorsqu'une norme européenne harmonisée n'atténue pas les risques recensés à la suite d'une analyse complète, qui se rapportent à l'une des exigences essentielles qu'elle vise à couvrir et qui s'appliquent aux produits relevant de son champ d'application, cette norme indique les risques non atténués et fournit, dans la mesure du possible, des informations non normatives sur les autres moyens de traiter ces risques.

Les normes harmonisées faisant l'objet de la demande comprennent au moins des dispositions relatives à la définition du problème de sécurité, aux objectifs de sécurité, à la spécification technique des exigences de sécurité et à la méthode d'évaluation.

En ce qui concerne la définition du problème de sécurité, les normes harmonisées faisant l'objet de la demande sont transparentes en ce qui concerne les menaces qu'elles couvrent, les

---

5 Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24, ELI: http://data.europa.eu/eli/dir/2006/42/oj.

6 Règlement (UE) 2023/1230 du Parlement européen et du Conseil du 14 juin 2023 sur les machines, abrogeant la directive 2006/42/CE du Parlement européen et du Conseil et la directive 73/361/CEE du Conseil (JO L 165 du 29.6.2023, p. 1, ELI: http://data.europa.eu/eli/reg/2023/1230/oj.

7 Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

8 Règlement (UE) 2023/1781 du Parlement européen et du Conseil du 13 septembre 2023 établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs et abrogeant le règlement (UE) 2021/694 (règlement sur les puces) (JO L 229 du 18.9.2023, p. 1), ELI: http://data.europa.eu/eli/reg/2023/1781/oj.

9 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

politiques et les hypothèses sur lesquelles elles se fondent, et aident les fabricants à identifier et à préciser les menaces, les politiques et les hypothèses. Cet objectif peut être atteint, par exemple, par le référencement de catalogues existants de contrôles de sécurité, de menaces, de méthodes d'attaque et de vulnérabilités, ou l'élaboration de tels catalogues, et par une discussion sur des hypothèses raisonnables.

Les objectifs de sécurité définissent le champ d'application du produit ou service cible et les propriétés de sécurité visées, sur la base des exigences essentielles énoncées dans le règlement sur la cyberrésilience. Les déclarations normatives figurant dans la norme harmonisée expriment de manière concise la solution envisagée aux risques identifiés (problème de sécurité). La méthode utilisée pour déterminer les objectifs de sécurité s'appuie sur les normes existantes définissant des approches d'analyse des risques. Les normes harmonisées devraient traiter de la relation entre les objectifs de sécurité et les risques identifiés (problème de sécurité).

La spécification des exigences de sécurité décrit le comportement souhaité en matière de cybersécurité attendu pour le produit ou service cible. Dans la mesure du possible, les normes couvrent divers niveaux de sécurité répondant aux différents besoins attendus du marché, tels que les finalités, les environnements opérationnels ou les catégories d'utilisateurs (par exemple, consommateurs, entreprises, utilisateurs critiques).

La méthode d'évaluation consiste en un ensemble de procédures d'évaluation requises pour apprécier l'objectif au regard des exigences des spécifications techniques définies précédemment. Il définit comment évaluer l'objectif afin d'attester le niveau de sécurité requis. Il couvre au moins la définition du concept de méthode d'évaluation, la définition du concept de méthode de composition (le cas échéant) et la définition des résultats d'évaluation escomptés.

Toutes les normes européennes harmonisées demandées élaborées en vertu de la présente décision sont rédigées de manière à faciliter leur publication au *Journal officiel de l'Union européenne*.

2. Exigences relatives à des normes européennes spécifiques

2.1 Normes horizontales de cybersécurité relatives aux propriétés des produits comportant des éléments numériques (entrées 1 à 14 de l'annexe I)

La définition de normes harmonisées horizontales portant sur différents aspects et mécanismes de la cybersécurité des produits soutient i) l'élaboration de nouvelles normes verticales harmonisées détaillées pour des produits ou des types de produits spécifiques, et ii) aide les fabricants à définir et à mettre en œuvre les exigences de sécurité applicables à leurs produits respectifs, y compris en particulier pour les produits qui ne sont pas couverts par des normes verticales existantes ou en projet. Les écarts par rapport aux normes harmonisées horizontales doivent dûment justifiés.

La norme européenne harmonisée relative à la conception, au développement et à la fabrication de produits comportant des éléments numériques de manière à garantir un niveau approprié de cybersécurité sur la base des risques (entrée 1 de l'annexe I) constitue un cadre couvrant tous les éléments définis à la section 1 de la présente annexe et énonce les principaux éléments qui doivent être abordés dans d'autres normes de sécurité des produits en lien avec le règlement sur la cyberrésilience.

Plutôt que de se concentrer sur les aspects communs minimaux, les normes harmonisées horizontales s'efforcent de fournir une vue d'ensemble large et utile des mécanismes de

sécurité pertinents qui peuvent s'appliquer aux produits relevant du champ d'application du règlement sur la cyberrésilience. Le cas échéant, les normes européennes harmonisées faisant l'objet de la demande comprennent des dispositions relatives au développement de logiciels sécurisés. La norme doit donc garantir la clarté du champ d'application de chaque déclaration normative.

Lors de l'examen de l'éventail des produits à couvrir dans le cadre du règlement sur la cyberrésilience aux fins de l'élaboration de normes horizontales, le CEN, le Cenelec et l'ETSI tiennent compte, le cas échéant, du fait que les exigences essentielles énoncées à l'annexe I de la proposition de règlement sur la cyberrésilience s'appliqueront aux produits comportant des éléments numériques qui relèvent également du champ d'application d'autres actes législatifs de l'Union, tels que les systèmes de dossiers informatisés de santé, les systèmes d'IA à haut risque au titre du règlement (UE) 2024/1689, les machines et produits connexes au titre de la directive nº 2006/42/CE du Parlement européen et du Conseil et le règlement (UE) 2023/1230, ou les puces électroniques fiables au titre du règlement (UE) 2023/1781.

2.2 Exigences en matière de traitement des vulnérabilités pour les produits comportant des éléments numériques (entrée 15 de l'annexe I)

La ou les normes européennes harmonisées relatives aux exigences de traitement des vulnérabilités prévoient des spécifications pour les processus de traitement des vulnérabilités, couvrant toutes les catégories de produits pertinentes, à mettre en place par les fabricants des produits comportant des éléments numériques. Ces procédés permettent aux fabricants:

(a) de recenser et documenter les vulnérabilités et les composants contenus dans leurs produits, notamment en établissant une nomenclature des logiciels dans un format couramment utilisé et lisible par machine couvrant au moins les dépendances de niveau supérieur du produit;

(b) s'agissant des risques posés aux produits comportant des éléments numériques, de gérer et corriger sans délai les vulnérabilités, notamment en fournissant des mises à jour de sécurité. Lorsque cela est techniquement possible, de nouvelles mises à jour de sécurité sont fournies séparément des mises à jour de fonctionnalité;

(c) de soumettre régulièrement les produits comportant des éléments numériques à des tests et examens de sécurité efficaces;

(d) dès la publication d'une mise à jour de sécurité, de divulguer publiquement des informations sur les vulnérabilités corrigées, en ce compris une description des vulnérabilités, des informations permettant aux utilisateurs d'identifier le produit concerné, les conséquences de ces vulnérabilités, leur gravité et des informations aidant les utilisateurs à y remédier. Dans des cas dûment justifiés, lorsque les fabricants considèrent que les risques pour la sécurité liés à la publication l'emportent sur les avantages en matière de sécurité, ils peuvent retarder la publication des informations relatives à une vulnérabilité corrigée jusqu'à ce que les utilisateurs aient eu la possibilité d'appliquer le correctif adapté;

(e) de mettre en place et d'appliquer une politique de divulgation coordonnée des vulnérabilités;

(f) de prendre des mesures pour faciliter le partage d'informations sur les vulnérabilités potentielles de leurs produits comportant des éléments numériques ainsi que des composants tiers contenus dans ces produits, y compris en fournissant une adresse de

contact pour le signalement des vulnérabilités découvertes dans les produits concernés;

(g) de prévoir des mécanismes permettant de distribuer en toute sécurité les mises à jour des produits comportant des éléments numériques afin de garantir que les vulnérabilités sont éliminées ou atténuées en temps utile et, au besoin, de manière automatique pour les mises à jour de sécurité;

(h) de veiller à ce que, lorsque des mises à jour de sécurité sont disponibles pour résoudre les problèmes de sécurité recensés, elles soient diffusées sans délai et, sauf accord contraire entre le fabricant et l'entreprise utilisatrice en ce qui concerne un produit sur mesure comportant des éléments numériques, gratuitement, accompagnées de messages de recommandation fournissant aux utilisateurs les informations pertinentes, y compris sur les mesures éventuelles à prendre.

2.3 Normes verticales de cybersécurité relatives aux propriétés des produits comportant des éléments numériques (entrées 16 à 41 de l'annexe I)

Les normes européennes harmonisées verticales relatives aux propriétés des produits comportant des éléments numériques fournissent des spécifications pour les exigences de cybersécurité applicables aux produits importants ou critiques tels que définis dans les annexes III et IV du règlement sur la cyberrésilience.

Des normes harmonisées verticales sont utilisées pour mettre en œuvre et développer les dispositions des normes horizontales faisant l'objet de la demande énumérées aux entrées 1 à 15 de l'annexe I, tout en tenant compte des différences pertinentes découlant de la destination et de l'utilisation raisonnablement prévisible. Compte tenu du calendrier des différents éléments livrables, les normes verticales garantissent la cohérence avec la norme horizontale relative à la conception, au développement et à la fabrication de produits comportant des éléments numériques de manière à garantir un niveau approprié de cybersécurité sur la base des risques (entrée 1 de l'annexe I) et, le cas échéant, avec la norme horizontale sur la gestion des vulnérabilités pour les produits comportant des éléments numériques (entrée 15 de l'annexe I). L'objectif d'alignement des normes verticales sur les normes horizontales énumérées aux entrées 2 à 14 de l'annexe I est également pris en considération, en escomptant une convergence des normes au cours du processus régulier de réexamen au fil du temps.

Pour les produits relevant de l'annexe IV du règlement sur la cyberrésilience pour lesquels il existe des domaines techniques ou des profils de protection, les normes harmonisées élaborées tiennent compte des schémas européens de certification de cybersécurité existants élaborés ou en cours d'élaboration au titre du règlement (UE) 2019/881, en particulier du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC).

Les normes harmonisées verticales élaborées pour la présente demande (entrées 16 à 41 de l'annexe I), axées spécifiquement sur les produits soumis à une évaluation de la conformité par un tiers (produits importants ou critiques), définissent une approche de l'assurance fondée sur les risques telle que les cas d'utilisation à faible risque peuvent n'être soumis qu'à de simples procédures de validation, tandis que les procédures de vérification applicables aux cas d'utilisation présentant un risque plus élevé seraient d'un niveau de plus en plus élevé.

Ces normes européennes harmonisées couvrent de manière adéquate les risques pertinents recensés pour une destination donnée ou une utilisation raisonnablement prévisible, et sont donc fondées sur une analyse complète des risques réalisée lors de l'élaboration de chaque norme harmonisée.

En outre, l'élaboration de normes harmonisées verticales couvrant un large éventail de produits ou de catégories de produits (tels que les technologies opérationnelles) peut soutenir et faciliter l'élaboration structurée et cohérente de normes harmonisées verticales spécifiques aux produits visées dans la présente demande, pour autant qu'il n'y ait aucune ambiguïté sur les exigences, le champ d'application, les risques couverts et les risques non couverts. Ces normes harmonisées verticales à large portée couvrent au moins une partie des risques associés à une destination spécifique et à une utilisation raisonnablement prévisible, et sont complétées par d'autres normes harmonisées verticales plus détaillées et spécifiques aux produits, visant à fournir une présomption de conformité pour un éventail de produits plus réduit, couvrant les risques supplémentaires ou spécifiques associés à ces produits et à leurs destinations pertinentes ainsi qu'à leurs utilisations raisonnablement prévisibles.