RAPPORT

sur les comptes annuels de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information relatifs à l'exercice 2014, accompagné de la réponse de l'Agence

(2015/C 409/25)

INTRODUCTION

1. L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ci-après «l'Agence» ou «l'ENISA»), sise à Athènes et à Héraklion ([1]), a été créée en vertu du règlement (CE) n° 460/2004 du Parlement européen et du Conseil ([2]), lequel, après plusieurs modifications, a été remplacé par le règlement (UE) n° 526/2013 du Parlement européen et du Conseil ([3]). La principale mission de l'Agence est de renforcer la capacité de l'Union à prévenir les problèmes de sécurité des réseaux et de l'information et, le cas échéant, à y faire face en s'appuyant sur les initiatives prises aux niveaux national et de l'Union européenne ([4]).

INFORMATIONS À L'APPUI DE LA DÉCLARATION D'ASSURANCE

2. L'approche d'audit choisie par la Cour comprend des procédures d'audit analytiques, des tests directs sur les opérations et une évaluation des contrôles clés des systèmes de contrôle et de surveillance de l'Agence. À cela s'ajoutent des éléments probants obtenus grâce aux travaux d'autres auditeurs ainsi qu'une analyse des prises de position de la direction.

DÉCLARATION D'ASSURANCE

3. Conformément aux dispositions de l'article 287 du traité sur le fonctionnement de l'Union européenne (TFUE), la Cour a contrôlé:

a) les comptes annuels de l'Agence, constitués des états financiers ([5]) et des états sur l'exécution du budget ([6]) pour l'exercice clos le 31 décembre 2014;

b) la légalité et la régularité des opérations sous-jacentes à ces comptes.

Responsabilité de la direction

4. La direction est responsable de l'établissement et de la présentation fidèle des comptes annuels de l'Agence ainsi que de la légalité et de la régularité des opérations sous-jacentes ([7]):

a) s'agissant des comptes annuels de l'Agence, la responsabilité de la direction comprend: la conception, la mise en œuvre et le maintien d'un système de contrôle interne pertinent pour l'établissement et la présentation fidèle d'états financiers exempts d'anomalies significatives, qu'elles résultent d'une fraude ou d'une erreur; le choix et l'application de méthodes comptables appropriées, sur la base des règles comptables adoptées par le comptable de la Commission ([8]); l'établissement d'estimations comptables raisonnables au regard de la situation du moment. Le directeur exécutif approuve les comptes annuels de l'Agence après que le comptable de celle-ci les a établis sur la base de toutes les informations disponibles, et qu'il a rédigé une note, accompagnant les comptes annuels, dans laquelle il déclare, entre autres, qu'il a obtenu une assurance raisonnable que ces comptes présentent, dans tous leurs aspects significatifs, une image fidèle de la situation financière de l'Agence;

b) s'agissant de la légalité et de la régularité des opérations sous-jacentes ainsi que de la conformité au principe de bonne gestion financière, la responsabilité de la direction consiste à assurer la conception, la mise en œuvre et le maintien d'un système de contrôle interne efficace et efficient, comprenant une surveillance adéquate et des mesures appropriées pour prévenir les irrégularités et les fraudes, et prévoyant, le cas échéant, des poursuites judiciaires en vue de recouvrer les montants indûment versés ou utilisés.

([1]) Le personnel opérationnel a été transféré à Athènes en mars 2013, tandis que le personnel administratif a été maintenu à Héraklion.
([2]) JO L 77 du 13.3.2004, p. 1.
([3]) JO L 165 du 18.6.2013, p. 41.
([4]) L'*annexe II* présente, de manière synthétique et à titre d'information, les compétences et activités de l'Agence.
([5]) Les états financiers comprennent le bilan, le compte de résultat, le tableau des flux de trésorerie, l'état de variation de l'actif net ainsi qu'une synthèse des principales méthodes comptables et d'autres notes explicatives.
([6]) Les états sur l'exécution du budget comprennent le compte de résultat de l'exécution budgétaire et son annexe.
([7]) Articles 39 et 50 du règlement délégué (UE) n° 1271/2013 de la Commission (JO L 328 du 7.12.2013, p. 42).
([8]) Les règles comptables adoptées par le comptable de la Commission sont fondées sur les normes comptables internationales pour le secteur public (IPSAS), publiées par la Fédération internationale des experts-comptables, ou, le cas échéant, sur les normes comptables internationales (IAS)/normes internationales d'information financière (IFRS), publiées par l'International Accounting Standards Board (IASB).

Responsabilité de l'auditeur

5. La responsabilité de la Cour consiste à fournir au Parlement européen et au Conseil ([9]), sur la base de son audit, une déclaration d'assurance concernant la fiabilité des comptes annuels de l'Agence ainsi que la légalité et la régularité des opérations sous-jacentes. La Cour conduit son audit conformément aux normes internationales d'audit et aux codes de déontologie de l'IFAC ainsi qu'aux normes internationales des institutions supérieures de contrôle établies par l'Intosai. En vertu de ces normes, la Cour est tenue de programmer et d'effectuer ses travaux d'audit de manière à pouvoir déterminer avec une assurance raisonnable si les comptes annuels sont exempts d'anomalies significatives et si les opérations sous-jacentes à ces comptes sont légales et régulières.

6. L'audit comprend la mise en œuvre de procédures en vue d'obtenir des éléments probants relatifs aux montants et aux informations qui figurent dans les comptes ainsi qu'à la légalité et à la régularité des opérations sous-jacentes. Le choix des procédures s'appuie sur le jugement de l'auditeur, qui se fonde sur une appréciation du risque que des anomalies significatives affectent les comptes et, s'agissant des opérations sous-jacentes, du risque de non-respect, dans une mesure significative, des obligations prévues par le cadre juridique de l'Union européenne, que cela soit dû à des fraudes ou à des erreurs. Lorsqu'il apprécie ces risques, l'auditeur examine les contrôles internes pertinents pour élaborer les comptes et assurer la fidélité de leur présentation, ainsi que les systèmes de contrôle et de surveillance visant à assurer la légalité et la régularité des opérations sous-jacentes, et il conçoit des procédures d'audit adaptées aux circonstances. L'audit comporte également l'appréciation de l'adéquation des méthodes comptables appliquées et de la vraisemblance des estimations comptables, ainsi que l'évaluation de la présentation générale des comptes. Lors de l'élaboration de son rapport et de sa déclaration d'assurance, la Cour a pris en considération les travaux d'audit réalisés par l'auditeur externe indépendant concernant les comptes de l'Agence, conformément aux dispositions de l'article 208, paragraphe 4, du règlement financier de l'Union européenne ([10]).

7. La Cour estime que les informations probantes obtenues sont suffisantes et appropriées pour étayer sa déclaration d'assurance.

Opinion sur la fiabilité des comptes

8. La Cour estime que les comptes annuels de l'Agence présentent fidèlement, dans tous leurs aspects significatifs, la situation financière de celle-ci au 31 décembre 2014 ainsi que les résultats de ses opérations et les flux de trésorerie pour l'exercice clos à cette date, conformément aux dispositions de son règlement financier et aux règles comptables adoptées par le comptable de la Commission.

Opinion sur la légalité et la régularité des opérations sous-jacentes aux comptes

9. La Cour estime que les opérations sous-jacentes aux comptes annuels relatifs à l'exercice clos le 31 décembre 2014 sont légales et régulières dans tous leurs aspects significatifs.

10. Les commentaires ci-après ne remettent pas en cause les opinions de la Cour.

COMMENTAIRES SUR LA GESTION BUDGÉTAIRE

11. Le niveau global des crédits engagés était élevé et a atteint 100 % (contre 94 % en 2013). Au total, 1,3 million d'euros de crédits engagés, soit 15 % du total des crédits, ont été reportés à 2015 (contre 1,2 million, soit 13,5 %, en 2013). S'agissant du titre II (dépenses administratives), le montant des reports de crédits engagés était élevé et a atteint 0,6 million d'euros, soit 49 % (contre 0,8 million d'euros, soit 59 %, en 2013). Ces reports s'expliquent par des investissements dans des infrastructures informatiques destinées aux deux sièges de l'Agence, commandées, comme prévu, en fin d'année.

SUIVI DES COMMENTAIRES DES ANNÉES PRÉCÉDENTES

12. L'*annexe I* donne une vue d'ensemble des mesures correctrices prises en réponse aux commentaires formulés les années précédentes par la Cour.

([9]) Article 107 du règlement délégué (UE) n° 1271/2013.
([10]) Règlement (UE, Euratom) n° 966/2012 du Parlement européen et du Conseil (JO L 298 du 26.10.2012, p. 1).

Le présent rapport a été adopté par la chambre IV, présidée par M. Milan Martin CVIKL, membre de la Cour des comptes, à Luxembourg en sa réunion du 8 septembre 2015.

Par la Cour des comptes

Vítor Manuel da SILVA CALDEIRA

Président

ANNEXE I

Suivi des commentaires des années précédentes

Année	Commentaires de la Cour	Mise en œuvre des mesures correctrices (Terminée/En cours/En attente/Sans objet)
2012	Le dernier inventaire physique complet des immobilisations remonte à 2009, alors que le règlement financier de l'Agence et ses modalités d'exécution en prévoient un au moins tous les trois ans.	En cours
2013	Le niveau global des crédits engagés a atteint 94 %, ce qui s'explique principalement par le fait que la demande de fonds supplémentaires adressée à la Commission pour financer le réaménagement des nouveaux bureaux à Athènes n'a été approuvée qu'en novembre 2013. Dans ce contexte, un montant de 0,5 million d'euros qui n'avait pas encore été engagé en fin d'exercice a été reporté en vertu d'une décision du conseil d'administration.	Sans objet
2013	Au total, 1,2 million d'euros de crédits (soit 13,5 % du total des crédits), engagés ou non, ont été reportés à 2014. Ces reports concernent principalement le titre II (dépenses administratives), pour lequel ils ont atteint 0,8 million d'euros, soit 59 % des crédits correspondant à ce titre. Ce chiffre élevé s'explique par le report de 0,5 million d'euros évoqué au point 11 et par un autre report de 0,3 million d'euros destiné à financer le mobilier et l'équipement de mise en réseau des bureaux d'Athènes, qui ont été commandés en fin d'année.	Sans objet
2013	Le personnel opérationnel de l'ENISA a été transféré à Athènes en 2013, tandis que le personnel administratif a été maintenu à Héraklion. Les coûts administratifs pourraient sans doute être réduits en regroupant l'ensemble du personnel sur un même site.	Sans objet
2013	En vertu du bail conclu entre les autorités grecques, l'Agence et le propriétaire, le loyer des bureaux d'Athènes est versé par les autorités grecques. Ce loyer est systématiquement versé avec un retard de plusieurs mois, ce qui constitue pour l'Agence un risque financier et un risque en matière de continuité de l'activité: ses opérations s'en trouveraient affectées et les investissements réalisés dans l'aménagement et les installations des bureaux seraient perdus si le propriétaire décidait de dénoncer le bail en raison des retards de paiement.	Terminée

ANNEXE II

Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (Athènes et Héraklion)

Compétences et activités

Domaines de compétence de l'Union selon le traité *(article 114 du traité sur le fonctionnement de l'Union européenne)*	Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire et après consultation du Comité économique et social, arrêtent les mesures relatives au rapprochement des dispositions législatives, réglementaires et administratives des États membres qui ont pour objet l'établissement et le fonctionnement du marché intérieur. La responsabilité en matière de marché intérieur relève d'une compétence partagée entre l'Union et les États membres [article 4, paragraphe 2, point a), du traité sur le fonctionnement de l'Union européenne].
Compétences de l'Agence *[règlement (UE) n° 526/2013 du Parlement européen et du Conseil]*	**Objectifs** 1. L'Agence acquiert et conserve un niveau élevé de compétences spécialisées. 2. L'Agence assiste les institutions, organes et organismes de l'Union dans l'élaboration des politiques de sécurité des réseaux et de l'information. 3. L'Agence assiste les institutions, organes et organismes de l'Union et les États membres dans la mise en œuvre des politiques nécessaires pour satisfaire aux exigences légales et réglementaires requises au titre des actes juridiques existants et à venir de l'Union en matière de sécurité des réseaux et de l'information, contribuant ainsi au bon fonctionnement du marché intérieur. 4. L'Agence aide l'Union et les États membres à améliorer et à renforcer leurs moyens et leur préparation pour prévenir les problèmes et incidents de sécurité des réseaux et de l'information, les détecter et y faire face. 5. L'Agence met à profit ses compétences spécialisées pour encourager une large coopération entre les acteurs des secteurs public et privé. **Tâches** 1. L'Agence accomplit les tâches suivantes: a) soutenir l'élaboration de la politique et du droit de l'Union en: i) apportant son concours et ses conseils sur toutes les questions relatives à la politique et au droit de l'Union en matière de sécurité des réseaux et de l'information; ii) fournissant des travaux préparatoires, des conseils et des analyses concernant l'élaboration et l'actualisation de la politique et du droit de l'Union en matière de sécurité des réseaux et de l'information; iii) analysant les stratégies en matière de sécurité des réseaux et de l'information accessibles au public et en favorisant leur publication; b) aider au renforcement des capacités en: i) soutenant les États membres, à leur demande, dans leurs efforts pour développer et améliorer la prévention, la détection et l'analyse des problèmes et incidents de sécurité des réseaux et de l'information et la capacité d'y faire face, et en leur fournissant les connaissances nécessaires; ii) promouvant et facilitant la coopération volontaire au sein des États membres, et entre les institutions, organes et organismes de l'Union et les États membres, dans leurs efforts pour prévenir et détecter les problèmes et les incidents de sécurité des réseaux et de l'information, et y faire face, lorsqu'ils ont une incidence transfrontière;

iii) assistant les institutions, organes et organismes de l'Union dans leurs efforts pour développer la prévention, la détection et l'analyse des problèmes et incidents de sécurité des réseaux et de l'information et la capacité d'y faire face, en particulier en soutenant le fonctionnement d'une équipe d'intervention en cas d'urgence informatique (CERT) à leur intention;

iv) soutenant le relèvement du niveau des capacités des CERT nationales, gouvernementales et de l'Union, y compris en favorisant le dialogue et l'échange d'informations, pour faire en sorte que, en ce qui concerne l'état de la technologie, chaque CERT satisfasse à un socle commun de capacités minimales et fonctionne selon les meilleures pratiques;

v) soutenant l'organisation et la réalisation d'exercices de l'Union portant sur la sécurité des réseaux et de l'information et, à leur demande, en conseillant les États membres en ce qui concerne les exercices nationaux;

vi) assistant les institutions, organes et organismes de l'Union et les États membres dans leurs efforts de collecte, d'analyse et, dans le respect des exigences des États membres en matière de sécurité, de diffusion des données sur la sécurité des réseaux et de l'information; et sur la base des informations fournies par les institutions, organes et organismes de l'Union et les États membres conformément aux dispositions du droit de l'Union et aux dispositions nationales arrêtées dans le respect du droit de l'Union, en tenant les institutions, organes et organismes de l'Union ainsi que les États membres informés du dernier état de la sécurité des réseaux et de l'information dans l'Union dans leur intérêt;

vii) aidant à la mise en place d'un mécanisme d'alerte rapide de l'Union qui soit complémentaire aux mécanismes des États membres;

viii) offrant une formation à la sécurité des réseaux et de l'information aux organismes publics compétents, le cas échéant en coopération avec les parties prenantes;

c) soutenir la coopération volontaire parmi les organismes publics compétents, et entre les parties prenantes, y compris les universités et les centres de recherche dans l'Union, ainsi que la sensibilisation, entre autres en:

i) favorisant la coopération entre les CERT nationales et gouvernementales ou les équipes de réaction aux incidents touchant la sécurité informatique (CSIRT), y compris la CERT pour les institutions, organes et organismes de l'Union;

ii) favorisant le développement et le partage des meilleures pratiques en vue d'atteindre un niveau avancé de sécurité des réseaux et de l'information;

iii) facilitant le dialogue et les efforts visant à développer et échanger les meilleures pratiques;

iv) favorisant les meilleures pratiques en matière de partage de l'information et de sensibilisation;

v) soutenant les institutions, organes et organismes de l'Union et, à leur demande, les États membres et leurs organismes concernés dans l'organisation d'activités de sensibilisation, y compris au niveau des utilisateurs individuels, et d'autres actions d'information pour accroître la sécurité des réseaux et de l'information et sa visibilité en définissant les meilleures pratiques et des lignes directrices;

d) soutenir la recherche et le développement ainsi que la normalisation en:

i) facilitant l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits, réseaux et services électroniques;

	ii) conseillant l'Union et les États membres sur les besoins en matière de recherche dans le domaine de la sécurité des réseaux et de l'information, en vue de pouvoir faire face efficacement aux risques et aux menaces actuels et émergents dans ce domaine, y compris en ce qui concerne les technologies de l'information et de la communication nouvelles et émergentes, et d'utiliser d'une manière efficace les technologies de prévention des risques; e) coopérer avec les institutions, organes et organismes de l'Union, y compris ceux qui traitent de la cybercriminalité et de la protection de la vie privée et des données à caractère personnel, pour aborder des questions d'intérêt commun, y compris en: i) échangeant savoir-faire et meilleures pratiques; ii) fournissant des conseils sur des aspects pertinents liés à la sécurité des réseaux et de l'information de manière à développer des synergies; f) contribuer aux efforts de l'Union pour coopérer avec les pays tiers et les organisations internationales, afin de promouvoir une coopération internationale sur les problèmes de sécurité des réseaux et de l'information, y compris en: i) s'impliquant en tant qu'observateur, le cas échéant, et en participant à l'organisation d'exercices internationaux, ainsi qu'en analysant et en rendant compte des résultats de ces exercices; ii) facilitant l'échange des meilleures pratiques des organisations concernées; iii) mettant des compétences spécialisées à la disposition des institutions de l'Union. 2. Les institutions, organes et organismes de l'Union et les organismes des États membres peuvent demander conseil à l'Agence en cas d'atteinte à la sécurité ou de perte d'intégrité ayant un impact significatif sur le fonctionnement des réseaux et des services. 3. L'Agence exécute les tâches qui lui sont assignées par des actes juridiques de l'Union. 4. L'Agence formule de manière indépendante ses propres conclusions, orientations et conseils sur des questions entrant dans le cadre du champ d'application et des objectifs du présent règlement.
Gouvernance	**Conseil d'administration** Le conseil d'administration est composé d'un représentant de chaque État membre et de deux représentants nommés par la Commission. Tous les représentants disposent du droit de vote. Chaque membre du conseil d'administration dispose d'un suppléant, qui le représente en cas d'absence.

	Les membres du conseil d'administration et leurs suppléants sont nommés sur la base de leur connaissance des tâches et des objectifs de l'Agence, en tenant compte des compétences nécessaires en matière de gestion et d'administration ainsi qu'en matière budgétaire pour s'acquitter des tâches incombant à un membre du conseil d'administration. Le mandat des membres du conseil d'administration et de leurs suppléants a une durée de quatre ans. Ce mandat est renouvelable. **Groupe permanent des parties prenantes** Le conseil d'administration crée, sur proposition du directeur exécutif, un groupe permanent des parties prenantes composé d'experts reconnus représentant les parties prenantes concernées, comme les entreprises du secteur des TIC, les fournisseurs de réseaux de communications électroniques ou de services accessibles au public, les organisations de consommateurs, les experts universitaires en matière de sécurité des réseaux et de l'information et les représentants des autorités réglementaires nationales notifiées au titre de la directive 2002/21/CE, ainsi que les autorités chargées du respect de la loi et de la vie privée. La durée du mandat des membres du groupe permanent des parties prenantes est de deux ans et demi. Le groupe permanent des parties prenantes conseille l'Agence dans l'exercice de ses activités. Il conseille en particulier le directeur exécutif lors de l'élaboration d'une proposition de programme de travail pour l'Agence ainsi que pour la communication avec les parties prenantes concernées sur toutes les questions liées au programme de travail. **Directeur exécutif** Le directeur exécutif est nommé par le conseil d'administration, pour un mandat de cinq ans renouvelable, sur la base d'une liste de candidats proposés par la Commission, à la suite d'une procédure de sélection ouverte et transparente. **Conseil exécutif** Le conseil exécutif est composé de cinq membres nommés parmi les membres du conseil d'administration, dont le président du conseil d'administration, qui peut également présider le conseil exécutif, et l'un des représentants de la Commission. **Audit externe** Cour des comptes européenne. **Audit interne** Service d'audit interne de la Commission européenne. **Autorité de décharge** Parlement européen, sur recommandation du Conseil.
Moyens mis à la disposition de l'Agence en 2014 *(2013)*	**Budget définitif** 9,7 millions d'euros *(9,7 millions d'euros)*, dont subvention de l'Union de 94 % *(93 %)*. **Effectifs au 31 décembre 2014** 48 *(47)* emplois prévus au tableau des effectifs, dont pourvus: 46 *(43)*. Autres emplois pourvus: 14 *(13)* agents contractuels et 2 *(3)* experts nationaux détachés. Total des effectifs: 62 *(59)*, dont affectés à des tâches: opérationnelles: 44 *(42)*, administratives: 18 *(17)*.

Produits et services fournis en 2014 *(2013)*	Les principales activités de l'ENISA pour 2014 ont été regroupées sous trois volets. **Volet** [1] **n° 1 — Soutien à l'élaboration des politiques de l'UE** En 2014, l'ENISA a soutenu le processus d'élaboration de politiques. Pour ce faire, elle a mis à la disposition des décideurs politiques des informations consolidées sur la nature des menaces émergentes et elle a formulé des messages clés à l'intention des États membres leur indiquant comment faire en sorte que leurs politiques et leurs capacités soient conformes aux objectifs de l'UE, compte tenu des enseignements tirés dans les différents États membres. Ces résultats reposaient sur le regroupement des sources d'informations disponibles dans un même contexte et, parallèlement, requéraient la collaboration et la participation d'importantes parties prenantes dans les domaines de l'évaluation des menaces, de l'atténuation des risques et de l'élaboration de politiques. Les objectifs et résultats suivants ont été atteints: — recensement des évolutions technologiques ainsi que des risques et des défis en la matière: mise en évidence des tendances, des défis en termes de sécurité, des risques correspondants et des contre-mesures requises, pour les technologies émergentes (avec une attention particulière accordée aux domaines/secteurs sélectionnés); — contribution aux initiatives politiques de l'UE: soutien aux initiatives politiques en apportant un éclairage sous l'angle de la sécurité ainsi qu'en recommandant des mesures de sécurité et des bonnes pratiques en termes de sécurité et de protection des données; — soutien à l'UE en matière d'éducation, de recherche et d'établissement de normes: renforcement de la collaboration et de la coopération, afin d'améliorer l'adoption de normes de sécurité et l'utilisation des résultats de la recherche en la matière; promotion de la sécurité des réseaux et de l'information (SRI) à tous les niveaux dans le domaine de l'éducation. Nombre de résultats: 10 *(7)* **Volet n° 2 — Soutien au renforcement des capacités** En 2014, l'Agence a réalisé un certain nombre d'activités destinées à aider ses principales parties prenantes à développer de nouvelles capacités opérationnelles et politiques pour faire face aux différents défis en matière de cybersécurité et élargir les capacités existantes. Les États membres de l'UE et les entreprises du secteur privé ont atteint des niveaux de maturité différents en ce qui concerne leur capacité à faire face à des cyberattaques et à des perturbations. Les activités réalisées par l'ENISA dans le cadre de ce volet visaient à relever le niveau de sécurité dans les États membres et le secteur privé, moyennant le recensement et la diffusion des bonnes pratiques auprès des secteurs public et privé et des citoyens européens en général. Les objectifs et, par suite, les résultats obtenus dans le cadre de ce volet étaient les suivants: — soutien au renforcement des capacités des États membres: aide aux États membres pour élaborer et harmoniser les stratégies nationales en matière de cybersécurité, les partenariats public-privé ainsi que les méthodologies de sécurité et les supports pédagogiques dans le domaine des CERT; — soutien au renforcement des capacités du secteur privé: élaboration de guides des meilleures pratiques, d'orientations, de recommandations minimales de sécurité ou d'orientations en matière d'harmonisation dans différents domaines de la sécurité des réseaux et de l'information [à savoir la sécurité des réseaux et de l'information et les marchés publics, la certification des réseaux intelligents, les systèmes ICS (systèmes de contrôles industriels)/SCADA (systèmes de surveillance et de saisie des données), les fournisseurs de services internet, l'informatique en nuage]; — amélioration du degré de préparation des citoyens de l'UE: mise à disposition d'orientations techniques, supports de diffusion d'informations et participation au mois européen de la cybersécurité.

	Nombre de résultats: 16 *(16)* **Volet n° 3 — Soutien à la coopération** La coopération est une condition préalable nécessaire à l'amélioration et au renforcement de la sécurité des réseaux et de l'information dans le marché unique européen ainsi qu'au développement des capacités SRI des États membres, des institutions de l'UE et des pays tiers. En 2014, l'ENISA a poursuivi ses travaux dans ce domaine en s'appuyant sur la collaboration existante mise en place dans les milieux concernés depuis la création de l'Agence. L'ENISA a soutenu la coopération en renforçant la confiance, en comblant l'écart entre les produits et services fournis sur le marché et les besoins ainsi qu'en mettant constamment à jour les informations fournies aux responsables de la mise en œuvre de la sécurité des réseaux et de l'information. En 2014, l'Agence a également soutenu la coopération en ce qui concerne le développement d'outils destinés à faciliter et à améliorer la communication internationale et l'échange mutuel de données pertinentes en matière de sécurité au sein de communautés partageant des intérêts communs dans différents États membres. Les objectifs et les résultats de ce volet étaient les suivants: — exercices de coopération en cas de crise: organisation de «Cyber Europe 2014»: planification et réalisation d'un exercice, établissement d'un rapport sur la coopération en cas de crise dans le domaine de la cybersécurité; — mise en œuvre de la législation de l'UE: élaboration de lignes directrices techniques et de mesures de sécurité en réponse aux rapports annuels d'incidents et recommandations 2013, afin de faire face aux incidents notables; — coopération régulière au sein des communautés SRI: mise à jour et renforcement des capacités opérationnelles des institutions des États membres en aidant la communauté des CERT à gagner en efficience et en efficacité. Nombre de résultats: 9 *(15)* REMARQUE: *certains résultats de 2014 ont donné lieu à plusieurs publications ou réalisations (par exemple les travaux correspondant au WP 3.2 D1 ont fait l'objet de six publications).*

([1]) En anglais: *work stream* (WS).

Source: annexe transmise par l'Agence.

RÉPONSE DE L'AGENCE

11. Un projet immobilier conséquent lié à la rénovation du bureau d'Athènes a été achevé fin décembre 2014. La durée d'achèvement des principaux travaux a été telle que des investissements complémentaires ou supplémentaires en infrastructures, essentiellement dans les locaux d'Athènes, ont dû être confiés à des contractants externes à la fin de l'année 2014. En conséquence, la livraison de ces investissements complémentaires a été programmée pour les premiers mois de l'année 2015, d'où le taux élevé de reports observé.