PROGRAMME DE TRAVAIL 2010

Exploiter les synergies - Produire un impact

VERSION FINALE – 9 NOVEMBRE 2009

Traduction. La version anglaise est la seule version officielle.

Table des matières

1 INTRODUCTION

Ce programme de travail définit et décrit les programmes thématiques pluriannuels(PTPA), les activités horizontales, les prestations de conseil et d'assistance et les activités administratives de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ci-après dénommée l'Agence) prévus pour 2010. Le programme de travail présente les principales tâches de l'Agence et le budget prévu pour ses activités en 2010.

1.1. Changements par rapport aux versions précédentes

La présente version du programme de travail est publiée afin de refléter une série de changements qui ont été convenus à la suite de l'arrivée du nouveau directeur exécutif de l'ENISA, le 16 octobre 2009. Ces changements peuvent être résumés comme suit:

- Réalignement organisationnel de l'ENISA, tel que communiqué au conseil d'administration le 3 novembre 2009.
- Attribution d'une plus grande priorité au PTPA 1 et recentrage sur les exigences de la communication de la Commission de mars 2009 (COM(2009)149).
- Retrait de l'Enquête paneuropéenne sur la sécurité de l'information du LT 2.1.
- Retrait du LT 3.3 (Application du «Cadre des risques émergents et futurs» avec les parties prenantes) du PTPA 3.
- Recentrage sur le renforcement de la préparation en matière de gestion nationale des risques dans le but de soutenir davantage le plan d'action relatif à la PIIC (LT 3.4).

Ces changements ont été opérés pour répondre à la demande des membres du conseil d'administration qui souhaitaient un recentrage sur les activités clés.

1.2. Cadre d'action

La communication de la Commission «i2010 – Une société de l'information pour la croissance et l'emploi»[1], a mis en lumière l'importance de la sécurité des réseaux et de l'information pour la création d'un espace européen unique de l'information. La disponibilité, la fiabilité et la sécurité des réseaux et des systèmes d'information sont de plus en plus primordiales pour nos économies et sociétés.

La Communication «Une stratégie pour une société de l'information sûre»[2] reconnaît qu'une société de l'information sûre doit être basée sur une sécurité des réseaux et de l'information (SRI) renforcée et une culture de la sécurité largement répandue. La seule façon d'y parvenir est une approche dynamique et intégrée, qui rassemble toutes les parties concernées et qui repose sur le dialogue, le partenariat et la responsabilisation. Face à la préoccupation des parties prenantes, il importe de reconnaître que la création d'une culture de la SRI est un défi pour tous.

[1] COM (2005) 229 du 01.06.2005.
[2] COM (2006) 251 du 31.05.2006.

Une résolution du Conseil[3] de décembre 2006 engage l'Agence à contribuer à la mise en œuvre de la stratégie de la Commission européenne dans le cadre de son mandat, tel qu'il est défini dans son règlement fondateur. L'ENISA répond à cette attente en alignant sa stratégie et ses plans de travail annuels sur la stratégie de la Commission européenne. En vue de maximiser l'impact de ses activités, l'Agence renforce les synergies et initiatives déjà existantes au niveau national et européen en suivant une approche ciblée et orientée vers des résultats.

La communication de la Commission de mars 2009[4] intitulée «Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité et la résilience» appelle l'ENISA à aider la Commission et les États membres à mettre en œuvre le plan d'action qui est proposé pour renforcer la sécurité et la résilience des IIC. Le présent programme de travail répond à cet appel essentiellement dans le contexte du PTPA 1 mais prévoit également d'appuyer le plan d'action avec des activités relevant des PTPA 1 et 2.

1.3. Principaux défis à relever

Parvenir à opposer une réponse cohérente aux menaces changeantes pesant sur la SRI, une réponse qui voit tous les acteurs contribuer à définir et à mettre en œuvre une approche globale de la sécurisation des infrastructures et de la réaction aux incidents de sécurité, reste le premier défi dans le domaine de la sécurité de l'information moderne car les esprits malveillants chercheront toujours à tirer parti du maillon le plus faible de tout système.

Une telle réponse nécessite une structure qui encourage l'action collaborative et permet à toutes les parties prenantes de travailler ensemble pour définir les priorités et moyens appropriés et, partant, assurer un degré adéquat de SRI dans l'UE. L'environnement d'applications extrêmement dynamique, qui ne cesse de se développer et d'offrir de nouveaux services aux entreprises et aux gouvernements, rend ce besoin encore plus pressant.

Toute tentative de définir et de mettre en œuvre une telle approche doit s'inscrire dans un contexte d'évolutions technologiques rapides comme la radio-identification (RFID), l'internet des objets ou l'internet du futur, tout en tenant compte d'autres tendances et défis importants tels que la cybercriminalité organisée et motivée par le lucre ou les cyberattaques à motivation politique.

Même si le défi technique consistant à réaliser de nouveaux progrès technologiques reste d'actualité, la priorité absolue concerne l'instauration d'une culture de la sécurité proactive. La création d'une telle culture appelle la prise en considération de plusieurs facteurs, parmi lesquels l'environnement multipartite, les lacunes éducatives, les modèles d'entreprise non optimisés, les déséquilibres entre les capacités des États membres, le rapprochement des législations et la dimension mondiale des questions de sécurité des réseaux et de l'information.

1.4. Rôle de l'ENISA

L'ENISA est dans une position unique pour prêter conseil et assistance aux États membres pour le renforcement de leurs capacités en matière de sécurité de l'information et des réseaux. Grâce à son indépendance, l'Agence peut fournir des conseils avisés et objectifs et jouer un important rôle de soutien de la Commission et des États membres pour faciliter les échanges de bonnes pratiques et d'informations entre toutes les parties prenantes à l'échelle européenne et maximiser ainsi les résultats et impacts de la SRI.

[3] 15768, 01.12.2006
[4] COM(2009) 149.

L'Agence soutient un dialogue multipartite ouvert et entretient, pour cela, des relations étroites avec l'industrie, le secteur universitaire et les utilisateurs. Elle établit et développe également des contacts avec un réseau de représentants nationaux (agents de liaison nationaux – ALN) et avec d'éminents experts individuels, réunis dans des groupes de travail ad hoc. Des interactions moins formelles, mais tout aussi efficaces, ont été également lancées par le biais de plates-formes et groupes d'experts virtuels en vue de collecter et de diffuser des recommandations d'experts et de faciliter l'échange d'informations avec et entre les secteurs public et privé.

La capacité de fournir des réponses rapides, indépendantes et de haute qualité aux demandes reçues des institutions européennes et des organismes compétents des États membres confère à l'Agence un rôle d'intermédiaire entre l'UE et les institutions nationales. Ce rôle est spécifique à l'ENISA et est actuellement unique au monde.

Une participation plus étroite au dialogue mené à l'échelle mondiale se développe actuellement grâce à l'élargissement constant des contacts avec des pays tiers de tous les continents ainsi qu'avec des institutions internationales (par ex. UIT, IETF, OASIS, OCDE). L'impact attendu est une meilleure intégration des avis d'importants acteurs étrangers et une promotion des approches européennes.

1.5. Planification pluriannuelle

En raison de son mandat et de ses ressources limitées, l'Agence a été invitée par le conseil d'administration à focaliser ses efforts sur un ensemble réaliste de priorités stratégiques. En concentrant ses efforts, l'Agence cherche à exercer un plus grand impact dans des domaines clés. Pour concrétiser cette ambition, elle entend stimuler les activités nationales et communautaires existantes, éviter les duplications d'efforts et maximiser les résultats. De telles activités européennes sont la recherche IST-FP6 pour la protection des infrastructures d'information critiques (PIIC), le programme-cadre pour l'innovation et la compétitivité (PIC), la priorité accordée aux TIC dans le 7e programme-cadre de recherche et de développement et le programme de fourniture interopérable de services européens d'administration en ligne aux administrations publiques, aux entreprises et aux citoyens (IDABC). Coopérer étroitement dans le cadre de ces initiatives, capitaliser leurs résultats, interagir avec les membres concernés et les amener à participer au travail de l'ENISA est l'un des éléments clés du présent programme de travail.

Pour obtenir l'impact souhaité et valoriser les synergies, l'Agence suit un plan de travail pluriannuel. L'un des principaux buts de cette approche concerne la mise en œuvre des orientations supérieures établies par le conseil d'administration de l'ENISA[5], tout en axant les efforts sur un éventail limité de priorités stratégiques, réunies sous le titre de programmes thématiques pluriannuels (PTPA). Ces programmes définissent le travail de l'Agence pour un certain nombre d'années. Un ensemble d'objectifs SMART[6] est défini pour chaque programme. Ces objectifs sont liés à des résultats et impacts souhaités et peuvent être évalués et suivis pendant la durée du

[5] Ces objectifs supérieurs sont les suivants:

- Développer la confiance dans la société de l'information en relevant le niveau de la SRI dans l'UE;
- Faciliter le marché intérieur des communications électroniques en aidant les institutions à choisir le dosage approprié de réglementations et d'autres mesures (en soulignant en particulier la contribution importante que peut apporter l'Agence à la directive-cadre);
- Renforcer le dialogue sur la SRI entre les diverses parties prenantes dans l'UE;
- Intensifier la coopération entre les États membres en vue de réduire leurs différences de capacités dans le domaine en question;

Appuyer les États membres et répondre à leurs demandes d'assistance.

[6] SMART est l'abréviation de spécifié, mesurable, acceptable, réaliste et situé dans le temps.

programme au moyen d'indicateurs clés de performance (ICP).

Chaque programme thématique est composé de plusieurs lots de travaux (LT) servant à la mise en œuvre des objectifs SMART du PTPA. Chaque lot de travaux définit les tâches à accomplir, les parties prenantes concernées, l'impact souhaité et les ressources requises.

Les lots de travaux peuvent être pluriannuels. Toutefois, étant donné que les PTPA sont mis en œuvre à travers les programmes de travail annuels de l'Agence, les ressources et les budgets indiqués ne peuvent se référer qu'aux actions, résultats et opérations pour une année. Le budget spécifié se réfère aux activités externes, telles qu'ateliers, conférences ou prestations d'expertise. Les indications concernant les ressources humaines se réfèrent aux efforts consentis par les experts de l'Agence.

Les programmes de travail peuvent aussi comporter des actions préparatoires (AP). Les actions préparatoires sont des activités conçues pour un an et servant à déterminer s'il convient de lancer un nouveau PTPA. Le feu vert ne peut être donné qu'une fois les résultats disponibles.

En 2008, l'Agence a commencé avec trois PTPA et une AP. En 2009, elle a mis l'accent sur les PTPA existants tout en intégrant le suivi de l'AP en tant que LT dans l'un des PTPA. Selon les conclusions de l'atelier informel qui a réuni le conseil d'administration et le groupe permanent des parties prenantes en juin 2009, l'Agence continuera à travailler sur ces trois PTPA en 2010 mais va également introduire deux nouvelles AP, qui seront décrites ici. La description complète des PTPA et des AP ainsi que des différents LT figure dans le chapitre suivant. Les LT proposés pour 2010 sont accompagnés de leurs propres objectifs SMART et des ICP qui sont considérés comme une première étape dans la réalisation des objectifs SMART correspondants.

PTPA 1: Améliorer la résilience des réseaux de communication électroniques européens

En 2008, ce PTPA s'est concentré sur l'inventaire, l'identification des bonnes pratiques et l'analyse des failles dans les mesures de sécurité déployées tant par les autorités réglementaires nationales (ARN) que par les opérateurs de réseaux et les fournisseurs de services. Le PTPA 1 a également analysé l'adéquation des technologies de dorsale internet actuellement déployées en ce qui a trait à l'intégrité et à la stabilité du réseau. En 2009, le PTPA 1 a comparé les résultats obtenus avec des expériences et résultats analogues acquis au niveau international, publié des lignes directrices et formulé des recommandations fondées sur un consensus, faisant suite à une vaste consultation menée avec les parties prenantes concernées. *En 2010, les principaux efforts dans ce domaine consisteront à soutenir les actions décrites dans la communication sur la PIIC publiée par la Commission en mars 2009.*

PTPA 2: Développer et entretenir la coopération entre les États membres

En 2008, ce PTPA a été consacré à: a) l'identification de cercles de compétences en matière de sécurité à l'échelle européenne sur des thèmes tels que la sensibilisation et la réponse aux incidents de sécurité et b) la facilitation de l'échange de bonnes pratiques de SRI au niveau européen[7]. En 2009, le thème du renforcement des capacités en matière de SRI pour les micro-entreprises y a été ajouté pour une durée d'un an. En 2010, une nouvelle coopération entre les États membres sera poursuivie et les possibilités de coopération internationale seront étudiées dans le but d'améliorer les capacités de tous les États membres et d'améliorer la cohérence globale de l'approche de la SRI au niveau paneuropéen. Étant donné ses ressources limitées, l'Agence coopérera étroitement avec les services de la Commission dans le but de minimiser ses efforts et de maximiser les résultats.

[7] Cette plate-forme fait suite au travail effectué en 2007 pour définir une feuille de route sur l'établissement d'un système européen d'échanges des bonnes pratiques en matière de SRI.

PTPA 3: Identifier les risques émergents afin d'instaurer la confiance

L'Agence a développé un cadre pour permettre aux décideurs de mieux comprendre et évaluer les risques émergents liés aux nouvelles technologies et aux nouvelles applications. L'un des principaux objectifs de ce cadre est d'aider les parties prenantes à tisser entre elles une relation de confiance pour ce qui concerne le traitement des risques émergents. À cet effet, l'Agence a développé en 2008 une preuve de concept d'une capacité européenne d'évaluation des risques susceptibles d'apparaître dans les deux à trois ans à venir, en liaison avec un Forum pour un dialogue multipartite avec les décideurs des secteurs public et privé. En 2009, cette preuve de concept a continué à être testée et développée en vue de son déploiement parmi les États membres en 2010. L'Agence continuera à préparer des rapports d'évaluation des risques afin d'y exprimer son avis sur les risques émergents liés aux nouvelles technologies et aux nouvelles applications. De plus, l'Agence explorera les thèmes liés à la responsabilité et à la confiance dans l'internet du futur. À ce titre, ce PTPA devrait remplir une fonction d'antenne pour les décideurs d'Europe et peut-être même au-delà.

AP 1: Identité, responsabilité et confiance dans l'internet du futur

Depuis les récentes évolutions de l'internet, chaque personne a la possibilité, en parallèle à sa vie réelle, de vivre des vies additionnelles dans le monde virtuel. Ces dernières années, on a observé une tendance, apparue d'abord dans la communauté de la recherche mais maintenant également dans les offres commerciales, à augmenter les interactions entre ces deux mondes, ce qui se traduit notamment par la possibilité d'accéder à des informations du monde réel par le biais de services internet. L'internet des objets (IdO), aussi en plein développement, est une évolution de la technologie moderne RFID qui consiste en réseaux de déclencheurs et nœuds de capteurs fonctionnant en interaction avec des objets munis d'étiquettes. En réponse à ces évolutions, l'objectif général de cette action préparatoire est de «veiller à ce que l'Europe maintienne un degré élevé de sécurité et de confiance parmi les utilisateurs et l'industrie concernant les infrastructures et les fournisseurs de services de TIC, tout en limitant les menaces susceptibles de peser sur les libertés civiles et la vie privée».

AP 2: Identification des moteurs et des cadres de la coopération sectorielle de l'UE en matière de SRI

Les actifs incorporels revêtent une valeur croissante pour les entreprises, il y a un besoin de plus en plus pressant d'actions économiques et opérationnelles générales incitant le développement de la coopération publique-privée pour relever les défis en matière de SRI. Comme les formes traditionnelles de protection ne suffisent plus à empêcher les intrus de s'introduire dans les systèmes pour y voler ou endommager des actifs clés, une approche plus proactive s'impose. Cette approche devrait comprendre un cadre global de différenciation organisationnelle entre les acteurs publics et privés concrétisée tout au long des chaînes d'approvisionnement organisationnelles, sur la base d'une évaluation réaliste des capacités des diverses parties à relever les défis de SRI, compte tenu de leurs responsabilités et capacités commerciales légitimes ou en tant que service public.

Le but de cette AP est de clarifier la question de savoir *comment* obtenir des acteurs pertinents l'engagement d'entreprendre une action collective pour relever les défis de SRI au niveau paneuropéen.

En plus de ce qui précède, l'Agence poursuivra un certain nombre d'activités horizontales, notamment de communication et de contact, le secrétariat des organes de l'ENISA, les relations avec les parties prenantes externes (organes de l'UE, États membres, industries, universités, consommateurs, institutions internationales et pays tiers), le développement des capacités internes, de la communication interne et du programme de travail de l'Agence.

De même, l'Agence continuera à prêter conseil et assistance en réponse aux demandes qui lui seront adressées. Enfin, le département administratif assurera l'administration générale de l'Agence, de ses finances, de ses ressources humaines, des TIC, des affaires juridiques et des achats. En ce qui concerne le développement des carrières de son personnel, l'Agence dispose d'un certain nombre d'instruments comprenant la classification, les promotions, les formations et des opportunités d'avancement professionnel au sein de l'Agence.

2 PROGRAMMES THÉMATIQUES PLURIANNUELS

2.1. PTPA 1: Améliorer la résilience des réseaux de communication électroniques européens

NOM DU THÈME:
PTPA 1: Améliorer la résilience des réseaux de communication électroniques européens
DESCRIPTION DU PROBLÈME À RÉSOUDRE
La disponibilité, l'intégrité et la continuité des réseaux publics de communication revêtent une importance majeure dans un environnement convergent d'infrastructures fixes et mobiles. La réalisation d'un environnement entièrement interconnecté et mis en réseau offre des possibilités importantes mais crée aussi des risques supplémentaires pour la sécurité. Avec la complexité grandissante des interdépendances, une perturbation dans une infrastructure peut facilement se propager dans d'autres infrastructures et avoir des répercussions à l'échelle européenne. En raison de la nature internationale des services de télécommunications, une approche commune s'avère nécessaire pour résoudre des questions telles que celles de la résilience et de la sécurité. Plusieurs États membres ont déjà élaboré des stratégies, politiques et initiatives réglementaires pour faire face au problème, ou sont en train de le faire. La plupart de ces stratégies sont basées sur la coopération ave les fournisseurs, l'échange d'informations sur les incidents et les menaces, l'élaboration de bonnes pratiques, le développement de mesures de préparation et l'exécution de tests au moyen d'exercices. Malgré ces efforts, la situation à travers l'Europe est très fragmentée en ce qui concerne les obligations et exigences à remplir pour assurer et renforcer la sécurité et la résilience des réseaux. Pour assurer le bon fonctionnement du marché intérieur et répondre aux demandes émanant des acteurs mondiaux il faut l'application de normes, règles et pratiques communes à travers l'UE. La récente communication COM(2009)149 de la Commission européenne reconnaît l'importance des réseaux de communication critiques et demande à l'ENISA de jouer un rôle actif pour veiller à ce que ces réseaux bénéficient d'une protection adéquate. Cette communication propose une série d'actions pour élaborer une approche intégrée au niveau de l'UE visant à renforcer la sécurité et la résilience des réseaux de communication critiques qui représenterait un complément et un apport de valeur ajoutée pour les programmes nationaux ainsi que pour les systèmes de coopération bilatérale et multilatérale entre les États membres. Pour chacune de ces activités, un engagement fort avec les secteurs privé et public est considéré comme un facteur clé de réussite. Les activités existantes seront renforcées si possible.
DESCRIPTION DE L'APPROCHE RETENUE POUR RÉSOUDRE LE PROBLÈME:
L'objectif du présent PTPA est d'aider les États membres et la Commission à améliorer la résilience des réseaux en «évaluant et améliorant collectivement la sécurité et la résilience dans les réseaux et services publics de télécommunications mobiles et fixes en Europe». En 2008, l'ENISA a exécuté une série d'exercices d'inventaire concernant les environnements réglementaires et stratégiques, les mesures prises par les fournisseurs et les normes et technologies existantes. En 2009, l'ENISA a analysé les conclusions de ces exercices d'inventaire, identifié les lacunes existant entre la situation actuelle et la situation recherchée, et collaboré avec les parties prenantes (à l'occasion d'ateliers, de réunions de travail d'experts, etc.) pour proposer les bonnes pratiques actuelles susceptibles de combler ces lacunes. En 2010, l'ENISA prévoit de mener les actions suivantes: 1) Aider les parties prenantes à déployer les guides ENISA de bonnes pratiques en matière de partage des informations et de signalement des incidents. L'Agence travaillera avec des parties prenantes

sélectionnées afin de mieux leur faire connaître les guides et recommandations de bonnes pratiques qui existent déjà. Il faudra pour cela débattre des conclusions et les valider au moyen d'ateliers et de groupes de travail thématiques, et apporter un soutien pour l'adoption des recommandations.

2) Aider les fournisseurs à améliorer la résilience de leurs réseaux. Il faudra pour cela analyser les obstacles juridiques et politiques au partage de l'information, identifier la métrique appropriée de la résilience et apporter des recommandations politiques dans le domaine des botnets.
3) Poursuivre le travail réalisé dans le domaine des protocoles de sécurité, notamment DNSSEC.
4) En collaboration avec des intervenants expérimentés dans ce domaine, élaborer un cadre holistique pour définir, mener et évaluer des exercices nationaux et, à long terme, transfrontaliers ou paneuropéens. Ce cadre sera accompagné d'une série de scénarios pour la conduite des exercices. Il reposera, entre autres, sur l'expérience de diverses parties prenantes, et visera à renforcer le rôle des CERT nationaux ou gouvernementaux dans la planification et l'exécution de ces exercices.

IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.)

Objectif SMART: D'ici à 2010, la Commission a fait usage des recommandations de l'ENISA dans le processus d'élaboration de ses politiques.	**ICP:** Commission (oui/non)
Objectif SMART: D'ici à 2012, au moins deux États membres participent à un exercice pilote utilisant le cadre.	**ICP:** # d'États membres
Objectif SMART: D'ici à 2010, au moins 50 % des États membres participent au forum paneuropéen.	**ICP:** % d'États membres
Objectif SMART: D'ici à 2012, au moins 50 % des États membres ont contribué au cadre.	**ICP:** % d'États membres, # de contributions

OBJECTIFS SUPÉRIEURS APPUYÉS PAR LE PROGRAMME

Développer la confiance dans la société de l'information en relevant le niveau de la SRI dans l'UE
Faciliter le marché intérieur des communications électroniques en aidant les institutions à choisir le dosage approprié de réglementations et d'autres mesures (en soulignant en particulier la contribution importante que peut apporter l'Agence à la directive-cadre). Renforcer le dialogue sur la SRI entre les diverses parties prenantes dans l'UE
Intensifier la coopération entre les États membres en vue de réduire leurs différences de capacités dans le domaine en question

PARTIES PRENANTES + BÉNÉFICIAIRES

Autorités réglementaires nationales, gouvernements d'États membres et responsables et décideurs de l'EU, CERT nationaux ou gouvernementaux, réseaux publics de communication et fournisseurs de services (téléphonie fixe, mobile et sur IP), fournisseurs d'accès internet (FAI), associations de fournisseurs (ECTA, ETNO, GSM Europe), points d'échange internet (Euro IX), associations d'audits (ISACA), fournisseurs de composantes de réseaux, de systèmes et de logiciels (EICTA)

POURQUOI L'ENISA?

Les cyberattaques massives et autres perturbations de grande envergure ne peuvent être contrées efficacement que sur une base multilatérale. Cela nécessite l'intégration de la législation, de la planification, des organisations, des infrastructures et des efforts techniques. Par sa désignation, l'ENISA est bien placée pour promouvoir et faciliter des politiques, activités et procédures conjointes dans ce domaine au niveau de l'Union européenne.

2.1.1 LT 1.1 - Aider les parties prenantes à déployer les guides ENISA de bonnes pratiques en matière de partage des informations et de signalement des incidents.

Nom du PTPA	
Améliorer la résilience des réseaux de communication électroniques européens	
NOM DU LOT DE TRAVAUX:	
LT 1.1: Aider les parties prenantes à déployer les guides ENISA de bonnes pratiques en matière de partage des informations et de signalement des incidents	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: Au moins 10 États membres participent aux débats sur le déploiement d'un système de partage des informations	**ICP:** # d'États membres
Objectif SMART: Au moins 10 États membres participent aux débats sur l'élaboration de mécanismes harmonisés de signalement des incidents	**ICP:** # d'États membres
Objectif SMART: Au moins 10 fournisseurs, petits et grands, participent aux débats sur l'élaboration de mécanismes harmonisés de signalement des incidents	**ICP:** # de fournisseurs
DESCRIPTION DES TÂCHES:	
En 2008, l'ENISA a réalisé une série d'exercices d'inventaire des questions réglementaires et politiques liées à la résilience et à la sécurité des réseaux. Se basant sur les conclusions de ces travaux, l'Agence, en coopération avec de nombreuses parties prenantes publiques et privées, a élaboré en 2009 des guides de bonnes pratiques concernant l'échange d'informations sur la sécurité des réseaux (NSIE) et les mécanismes de notification des incidents. Ces guides de bonnes pratiques sont le fruit d'une coopération avec une large gamme de parties prenantes, qui ont longuement examiné puis validé les guides de l'ENISA à l'occasion d'un ou plusieurs ateliers thématiques et d'un processus de consultation ouvert. Le principal objectif de ce lot de travaux est d'identifier les incitations susceptibles d'encourager les parties prenantes publiques et privées à déployer les guides de bonnes pratiques identifiées par l'ENISA et ses parties prenantes ainsi que de travailler avec eux pour approfondir leur compréhension des recommandations essentielles. L'Agence fera la promotion des résultats déjà engrangés, débattra des conclusions avec les parties prenantes concernées, validera ces conclusions à l'occasion d'ateliers ciblés et de réunions de groupes de travail thématiques, et responsabilisera les parties prenantes dans leurs efforts d'adoption des recommandations. Dans le domaine du partage des informations, l'Agence vise à: 1) augmenter le nombre de pays qui mettent en place et gèrent un NSIE en Europe; 2) soutenir le développement du Forum européen pour le partage d'information entre États membres (évoqué par la communication COM(2009)149), qui deviendrait le premier NSIE paneuropéen. À cet égard, l'ENISA organisera des ateliers ciblés afin de promouvoir ces guides de bonnes pratiques auprès de tous les États membres. L'Agence favorisera un dialogue entre experts, mobilisera les parties prenantes publiques et privées, veillera à leur participation au processus, validera les conclusions précitées et prêtera assistance aux États membres en organisant des formations, cela pour promouvoir la mise en place et la gestion d'une plate-forme de partage des informations. En parallèle, rassemblera les principaux NSIE de l'Europe ainsi que les projets nationaux et paneuropéens dans ce domaine afin de débattre de la possibilité de constituer la première plate-forme européenne. Les activités proposées par l'ENISA concernant l'échange d'informations sur la sécurité des réseaux seront à l'ordre du jour des débats permanents qui ont été lancés par la Commission européenne au sujet de la mise en place d'un partenariat public-privé européen pour la résilience (EP3R), comme évoqué dans son plan d'action en matière de protection des IIC (COM(2009)149).	

Pour ce qui est des mécanismes de notification des incidents, l'ENISA identifiera les parties prenantes concernées, tant publiques que privées, et travaillera avec elles afin de favoriser un dialogue ouvert. Ce projet est conforme aux dispositions du nouveau «cadre réglementaire commun pour les réseaux et services de communications électroniques» relatif à l'intégrité et à la disponibilité des réseaux publics de communication [voir par ex. l'article 13, paragraphe a), de la directive «cadre» 2002/21/CE].

L'ENISA, par un dialogue structuré avec les parties prenantes publiques et privées, élaborera des lignes directrices concrètes et réalistes sur l'éventuelle mise en œuvre de ces dispositions (par ex. pour les atteintes à la sécurité, la perte d'intégrité ou la liste annuelle consolidée des incidents). L'Agence assurera une validation intensive et étendue de ses recommandations et veillera à ce que celles-ci soient largement acceptées. La mise en œuvre des guides de bonnes pratiques – dont l'ENISA fait la promotion – dans les phases initiales du paquet réglementaire sur les télécommunications encouragera l'harmonisation des processus et politiques aux niveaux national et paneuropéen.

L'ENISA continuera à travailler, en coopération avec toutes les parties prenantes publiques et privées concernées, sur l'élaboration de mesures et de politiques susceptibles d'améliorer l'intégrité des offres des réseaux et services.

RÉSULTATS ET CALENDRIER:

Atelier thématique et formation sur les échanges d'informations sur la sécurité des réseaux (2e-3e trimestre 2010)
Rapport d'avancement sur l'échange d'informations sur la sécurité des réseaux en Europe (4e trimestre 2010)
Deux ateliers thématiques sur les mécanismes de signalement des incidents (1er-3e trimestre 2010)
Projet de lignes directrices sur la mise en œuvre d'un système de notification des incidents majeurs (4e trimestre 2010)

PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:

Les parties prenantes possibles englobent les ARN, les autorités politiques nationales compétentes en matière de résilience des réseaux et services publics de communication, les associations du secteur (EICTA, ETNO, EUROISPA, GSM Europe, ISACA, Euro-IX), les opérateurs de télécommunications (téléphonie fixe, mobile et sur IP) et les fournisseurs d'accès internet (FAI).

RESSOURCES POUR 2010 (personnes-mois et budget)

- 100 000 euros
- 11,5 personnes-mois

LOT DE TRAVAUX PROPOSÉ PAR:

ENISA

BASE JURIDIQUE

Règlement ENISA, article 3, points a), c), d), f) et k)

2.1.2 L.T. 1.2 – Aider les fournisseurs à améliorer la résilience de leurs réseaux

Nom du PTPA	
Améliorer la résilience des réseaux de communication électroniques européens	
NOM DU LOT DE TRAVAUX:	
LT 1.2: Aider les fournisseurs à améliorer la résilience de leurs réseaux	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: Au moins 10 États membres et 10 grandes parties prenantes privées participent aux débats sur les obstacles juridiques et politiques	ICP: # d'États membres, # de fournisseurs
Objectif SMART: Au moins 10 États membres et 10 grandes parties prenantes privées participent aux débats sur la métrique et les techniques de mesure	ICP: # d'États membres, # de fournisseurs
Objectif SMART: Au moins 10 États membres et 10 grands FAI/IX participent aux débats sur la métrique et les techniques de mesure	ICP: # d'États membres, # de fournisseurs
DESCRIPTION DES TÂCHES:	
En 2008, l'ENISA a réalisé un exercice d'inventaire des mesures prises par les fournisseurs concernant la résilience et la sécurité de leurs réseaux; en 2009, elle a élaboré une série de recommandations et de bonnes pratiques sur divers thèmes. Ces thèmes sont notamment les obstacles juridiques et politiques interdisant aux fournisseurs de partager des informations sur des questions sensibles, les moyens efficaces de mesurer la résilience et la sécurité des fournisseurs, et les politiques efficaces pour lutter contre les botnets. Les obstacles juridiques et politiques entravent considérablement la capacité des opérateurs privés à échanger des informations avec les parties prenantes concernées. On ne voit pas encore bien comment les lois ou politiques régissant des questions telles que la protection de la vie privée et des données s'appliqueraient aux réseaux d'information, ou comment l'obligation de confidentialité s'appliquerait aux partenariats public-privé dans le domaine de la protection des infrastructures d'information critiques (PIIC). La plupart de ces lois ont été adoptées avant l'émergence de la société de l'information et la dépendance aux réseaux d'information. Nous continuons à manquer d'un cadre clair permettant d'échanger efficacement et en temps utile les informations sur la protection des infrastructures critiques, notamment une divulgation responsable et rapide des vulnérabilités. La présente activité cherchera à identifier ces failles des lois et politiques pour qu'il devienne possible d'évaluer l'ampleur de leurs effets sur le déploiement efficace de l'échange d'informations dans le domaine de la protection des infrastructures d'information critiques. Malgré l'abondance de politiques, mesures et méthodologies couvrant la totalité du cycle de vie des incidents de sécurité et de résilience, il n'existe pas de moyen adéquat pour mesurer la résilience et la sécurité des réseaux. Des travaux considérables ont été réalisés en matière de métrique et de techniques de mesure concernant la disponibilité et l'intégrité de réseaux particuliers, notamment des accords sur les niveaux de service. La plupart de ces travaux n'abordent pas le problème d'une façon holistique ni selon une perspective politique. Il est encore vrai que les responsabilités politiques et les régulateurs ne disposent pas d'un mécanisme clair pour mesurer la résilience et la sécurité des réseaux publics de communications, comme en témoigne le manque de métrique fiable. L'ENISA entend rassembler toutes les parties prenantes concernées (industrie, universités, décideurs politiques, organisations internationales, organismes de normalisation) afin d'analyser ce domaine, d'identifier les tendances actuelles et projets pertinents (ex.: le projet **AMBER**, financé par l'UE) et de travailler avec ces parties prenantes pour définir les techniques appropriées aux mesures et à la métrique associée en matière de résilience. De plus, à long terme, l'ENISA cherchera à établir une série d'indicateurs clés de performance nationaux et, par la suite, paneuropéens susceptibles de mesurer la résilience et la sécurité de nos réseaux publics de communication. Les botnets ont été identifiés comme une menace majeure pesant sur internet et, par conséquent, sur nos services critiques de communication. Leur degré de prolifération et de pénétration est extrêmement élevé dans les ordinateurs individuels. L'ENISA étudiera le phénomène des botnets, fera l'inventaire des politiques nationales en la matière, travaillera en collaboration avec les parties prenantes concernées (FAI, IX, EuroISPA, EuroIXs, ETNO, etc.) sur une série de recommandations politiques, et élaborera des suggestions concrètes relatives à des techniques de mesure cohérentes et applicables. L'ENISA vise à consulter ouvertement toutes les parties prenantes concernées	

sur les aspects de coopération possibles au niveau paneuropéen (assistance mutuelle, partage des informations, etc.).
RÉSULTATS ET CALENDRIER:
Obstacles juridiques et politiques au partage d'informations sensibles dans le contexte de la PIIC (3e trimestre 2010) Analyse pointue de la métrique et des techniques de mesure (4e trimestre 2010) Botnets: recommandations politiques (4e trimestre 2010)
PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:
ARN, les autorités politiques nationales compétentes en matière de résilience des réseaux et services publics de communication, les associations du secteur (EICTA, ETNO, EUROISPA, GSM Europe, ISACA, Euro-IX), les opérateurs de télécommunications (téléphonie fixe, mobile et sur IP) et les fournisseurs d'accès internet (FAI)
RESSOURCES POUR 2010 (personnes-mois et budget)
• 150 000 euros • 13,5 personnes-mois
LOT DE TRAVAUX PROPOSÉ PAR:
ENISA
BASE JURIDIQUE
Règlement ENISA, article 3, points a), c), d), f) et k)

2.1.3 L.T. 1.3 – Examen d'actions innovantes

Nom du PTPA:		
Améliorer la résilience des réseaux de communication électroniques européens		
NOM DU LOT DE TRAVAUX:		
L.T. 1.3: Examen d'actions innovantes		
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):		
Objectif SMART: Au moins 10 acteurs du secteur participent au projet pilote d'application des recommandations/lignes directrices émises en vue du déploiement du protocole DNSSEC	**ICP:**	# d'acteurs du secteur
Objectif SMART: Couverture d'au moins 200 millions d'utilisateurs par les opérateurs interrogés dans l'évaluation d'impact des protocoles de routage	**ICP:**	# d'utilisateurs
Objectif SMART: Au moins 10 acteurs du secteur valident le rapport sur les principes de conception d'architecture qui se traduisent par une véritable sécurité de bout en bout (e2e)	**ICP:**	# d'acteurs du secteur
Objectif SMART: Organisation d'un atelier «Porte ouverte aux technologies qui améliorent la résilience des réseaux» à l'intention des agents scientifiques de la Commission européenne, avec des participants de parties prenantes de tous les secteurs (vendeurs, opérateurs, régulateurs, utilisateurs finals, etc.). Au moins 30 participants et 3 secteurs représentés.	**ICP:**	**#** de participants # de secteurs participants
DESCRIPTION DU LOT DE TRAVAUX		
En 2008 et 2009, l'ENISA a analysé une série de technologies, protocoles et architectures (notamment IPv6, Multiprotocol Label Switching et DNS Security Extensions) afin de déterminer leur potentiel d'amélioration de la résilience des réseaux publics de communication. Dans ce contexte, des incitations concernant des aspects relatifs aux marchés et/ou aux politiques ont été examinées sur le plan de leur impact sur les pratiques commerciales. Des recommandations et guides de bonnes pratiques ont été élaborés principalement à l'intention des décideurs de l'UE et du niveau national. Sans se limiter aux technologies, architectures et protocoles, l'Agence a également évalué l'impact de l'évolution des technologies de mise en réseau («informatique dans le nuage», réseaux de capteurs, systèmes de détection et de diagnostic en ligne, etc.) sur la sécurité et la disponibilité des ressources en matière de réseaux, et a élaboré des lignes directrices applicables aux futures recherches. Ces tâches ont été réalisées en étroite collaboration avec deux groupes d'experts composés d'acteurs issus de tous les secteurs concernés. Sur la base de son expérience en 2009, l'Agence continuera à travailler avec ces deux groupes d'experts. En 2009, l'ENISA a élaboré des guides de bonnes pratiques pour le déploiement du protocole DNSSEC. Elle a présenté les principales considérations à prendre en compte par les fournisseurs qui déploient cette technologie, ainsi que les éléments à inclure dans les déclarations de politiques et de pratiques pour les Trust Anchor Repositories. Le principal objectif de ce lot de travaux est de tester ou déployer les recommandations dans des environnements de travail réel, cela afin d'obtenir des informations en retour sur leur efficacité, validité et adéquation. L'ENISA compte promouvoir largement ces recommandations, qui s'adressent surtout aux décideurs de l'UE et du niveau national, afin de favoriser l'adoption la plus rapide des actions innovantes les plus prometteuses. De même, l'expérience acquise dans ce domaine aidera la section Sensibilisation de l'Agence à préparer une campagne d'information, destinée aux utilisateurs ou à des groupes d'utilisateurs spécifiques, sur les risques des protocoles DNS et DNSSEC dans le cadre des applications ordinaires de navigation internet telles que services bancaires, shopping, etc.		

Assurer le DNS est un élément du processus à suivre pour atteindre un degré élevé de résilience et de sécurité dans les réseaux publics de communication. Au sein des réseaux publics de communication, une autre infrastructure cruciale qui se doit d'être résiliente est l'infrastructure de routage. À cet égard, l'ENISA vise à évaluer l'impact du déploiement de technologies de routage résilientes. Cette évaluation servira à élaborer des lignes directrices/recommandations sur ce déploiement destinées en particulier aux décideurs.

En parallèle à ces activités, l'ENISA étendra son travail sur l'évaluation de l'impact des tendances de la mise en réseau pour couvrir également la résilience des réseaux publics de communication, cela en identifiant et en veillant à promouvoir des principes de conception d'architecture qui se traduisent par une véritable sécurité de bout en bout (e2e). Dans un premier temps, l'accent avait été placé sur les technologies de la couche transport des réseaux de communication. Toutefois, les réseaux publics de communication forment la base sur laquelle une pléthore d'applications/services est offerte par le biais des fournisseurs d'accès qui, dans de nombreux cas, sont indépendants de l'opérateur du réseau. À cet égard, ce qui présente de l'intérêt pour les utilisateurs des services TIC, c'est la résilience et la sécurité e2e et non pas seulement un réseau de transport résilient et sûr. Plutôt que chercher à identifier des architectures performantes, il est plus utile d'identifier les principes de conception. Les architectures individuelles sont parfois fortement liées aux spécificités des technologies qu'elles déploient, tandis que les principes sont susceptibles de rester les mêmes quelle que soit la technologie utilisée.

Enfin, ces activités seront également combinées avec un atelier ciblé intitulé «Porte ouverte aux technologies qui améliorent la résilience des réseaux». Le but de cette activité est de donner aux agents scientifiques de la Commission européenne (DG INFSO, JLS, MARKT et Recherche) un aperçu du sujet de la résilience des réseaux de communication et des activités de l'ENISA dans ce domaine. Sur la base de l'expérience accumulée en 2009, cette activité pourrait être étendue au-delà du domaine du L.T. 1.3 (technologies) pour couvrir tous les aspects du PTPA 1 (y compris les politiques).

RÉSULTATS ET CALENDRIER:

Plan préparatoire pour une campagne d'information, destinée aux utilisateurs ou à des groupes d'utilisateurs spécifiques, sur les risques des protocoles DNS et DNSSEC dans le cadre des applications ordinaires de navigation internet telles que services bancaires, shopping, etc. (3e trimestre 2010)
Rapport sur le(s) projet(s) pilote(s) de promotion du travail du L.T. 1.3 de 2008-2009 sur le thème «Améliorer la résilience du DNS» (4e trimestre 2010)
Évaluation de l'impact du déploiement des technologies de routage à résilience et élaboration de lignes directrices/recommandations (4e trimestre 2010)
Rapport sur les principes de conception d'architecture qui se traduisent par des réseaux publics de communication véritablement résilients et sûrs de bout en bout (e2e) (4e trimestre 2010)
Atelier «Porte ouverte aux technologies qui améliorent la résilience des réseaux» (4e trimestre 2010)

PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:

Vendeurs d'équipement de mise en réseau, autorités réglementaires nationales (ARN), opérateurs de réseaux, opérateurs de réseaux virtuels, experts en matière de technologies dorsales et internet résilientes, institutions de R&D industrielles, universités et centres de recherche, plates-formes technologiques européennes (par ex. eMobility, NEM, NESSI, etc.).

RESSOURCES POUR 2009 (personnes-mois et budget)

- 195 000 euros (ateliers, expertise-conseil, gestion des groupes d'experts, publications électroniques et imprimées).
- 17,5 personnes-mois

LOT DE TRAVAUX PROPOSÉ PAR:

ENISA

BASE JURIDIQUE

Règlement ENISA, article 3, points a), b), c), f) et k)

2.1.4 L.T. 1.4 – Responsabiliser les parties prenantes en vue du premier exercice paneuropéen

Nom du PTPA:	
Améliorer la résilience des réseaux de communication électroniques européens	
NOM DU LOT DE TRAVAUX:	
L.T. 1.4: Responsabiliser les parties prenantes en vue du premier exercice paneuropéen	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: Au moins 50 % des États membres participent aux débats sur le premier exercice paneuropéen	**ICP:** % d'États membres
Objectif SMART: Au moins 3 États membres appliquent le guide de bonnes pratiques en matière d'exercices de l'ENISA	**ICP:** # d'exercices
Objectif SMART: Au moins 30 % des États membres expriment leur soutien au cadre de l'ENISA relatif à la réalisation d'exercices	**ICP:** % d'États membres
DESCRIPTION DES TÂCHES:	

Le guide de bonnes pratiques en matière d'exercices de l'ENISA révèle l'importance des exercices pour vérifier l'adoption de certaines mesures de préparation aux urgences par les parties prenantes publiques et privées. La récente communication sur la PIIC souligne l'importance des exercices pour améliorer les mesures de préparation aux urgences. À ce jour, seul un petit nombre d'États membres ont réalisé des exercices pour tester leurs mesures de préparation.

Dans le contexte de ce lot de travaux, l'ENISA vise à faciliter le dialogue au niveau paneuropéen concernant ces exercices. L'Agence aidera les États membres à réunir des parties prenantes susceptibles de travailler ensemble à la conception, au développement, à la mise en œuvre et à l'évaluation du premier exercice paneuropéen. Dans ce but, l'ENISA, en étroite coopération avec la Commission et les États membres, assurera une collaboration efficace avec toutes les parties prenantes et projets paneuropéens concernés (par ex. les projets financés par le programme EPCIP).

Il s'agira de travailler avec les parties prenantes pour mieux leur faire connaître les guides de bonnes pratiques relatifs aux exercices nationaux, d'en valider les contenus à l'occasion de débats ciblés et de réunions de groupes de travail thématiques, et enfin d'aider les parties prenantes à participer au premier exercice paneuropéen.

Par ce dialogue, l'ENISA tâchera d'élaborer une série de scénarios possibles à utiliser pour la réalisation des premiers exercices paneuropéens (par ex. l'identification des voies critiques), et de proposer un cadre holistique pour mener des exercices aux niveaux national, transfrontalier ou même paneuropéen. Ce cadre et les scénarios possibles permettront aux parties prenantes publiques et privées de définir, organiser et réaliser des exercices sur l'état de préparation. Les composantes possibles du cadre sont notamment les profils des parties prenantes (publics cibles et organisateurs), le type d'exercices, les mesures de l'état de préparation à tester, les scénarios possibles, les méthodologiques d'évaluation, etc. L'ENISA validera le cadre proposé et les scénarios possibles à l'occasion d'un atelier thématique et d'une interaction avec des experts.

Dans ce contexte, l'ENISA continuera à collaborer avec les activités et projets liés aux questions de préparation aux cas d'urgence. L'Agence collaborera avec une étude financée par le programme EPCIP qui évaluera l'état de préparation en Europe ainsi que les futures politiques, mesures et orientations susceptibles d'améliorer cet état de préparation et la coopération européenne au sein du secteur des télécommunications. De plus, l'ENISA continuera à travailler avec la Commission et les États membres de l'UE à la mise en œuvre des actions prévues dans la communication «Renforcer la capacité de réaction de l'Union aux catastrophes» (COM(2008) 130). L'ENISA, en coopération avec les parties prenantes concernées, facilitera un dialogue sur l'amélioration de la coopération, du partage d'informations et de l'assistance mutuelle entre parties prenantes en cas de réaction à une catastrophe dans le secteur des télécommunications. Sur la base des conclusions et résultats de ces actions, l'ENISA recueillera l'avis de ses parties prenantes sur les prochaines étapes possibles dans le domaine de la préparation aux cas d'urgence et du rétablissement après catastrophe. L'ENISA utilisera ces avis pour formuler une série de recommandations politiques relatives au travail restant à accomplir en matière de préparation aux cas d'urgence et de rétablissement après catastrophe.

RÉSULTATS ET CALENDRIER:
Atelier(s) thématique(s) sur le cadre d'exercices (2e trimestre 2010) Cadre pour la réalisation d'exercices (4e trimestre 2010) Recommandations politiques relatives à la préparation aux cas d'urgence et au rétablissement après catastrophe
PARTIES PRENANTES
ARN, les autorités politiques nationales compétentes en matière de résilience des réseaux et services publics de communication, les associations du secteur (EICTA, ETNO, EUROISPA, GSM Europe, ISACA, Euro-IX), les opérateurs de télécommunications (téléphonie fixe, mobile et sur IP) et les fournisseurs d'accès internet (FAI), Commission européenne, communautés CERT
RESSOURCES POUR 2010 (personnes-mois et budget)
• 100 000 euros • 13,5 personnes-mois
LOT DE TRAVAUX PROPOSÉ PAR:
ENISA, conseil d'administration, Commission
BASE JURIDIQUE
Règlement ENISA, article 3, points a), c), d), f) et k)

2.2. PTPA 2: Développer et entretenir des modèles de coopération

NOM DU THÈME:
PTPA 2: Développer et entretenir des modèles de coopération
DESCRIPTION DU PROBLÈME À RÉSOUDRE
Beaucoup d'États membres ont besoin de renforcer leurs capacités dans divers domaines de la sécurité des réseaux et de l'information (SRI). Plusieurs États membres coopèrent déjà en échangeant des informations sur les bonnes pratiques, mais ils ne le font pas sur une base structurée. Ainsi se perdent des opportunités de créer des synergies et d'améliorer l'efficience et l'efficacité de la SRI à l'échelle européenne.
DESCRIPTION DE L'APPROCHE RETENUE POUR RÉSOUDRE LE PROBLÈME:
Avec ce PTPA, l'ENISA répondra à ces besoins en renforçant son rôle de facilitateur, de centre d'expertise et d'intermédiaire pour la fourniture de conseils. Les experts techniques de l'ENISA élaboreront divers modèles de coopération dans des domaines prédéfinis (sensibilisation, réaction aux incidents et renforcement des capacités de SRI pour les micro-entreprises) en s'inspirant des travaux déjà réalisés. De plus, l'Agence continuera à développer l'échange de bonnes pratiques en SRI au niveau européen, incluant des outils de soutien tels que la plate-forme de dialogue en ligne, le répertoire Who-is-Who, les fiches pays et les rapports pays sur les activités réalisées dans les États membres. Particulièrement importants seront les différents ateliers thématiques qui serviront à renforcer les relations avec des communautés existantes de SRI (par ex. CERT) ou créer de nouvelles communautés partageant des intérêts communs dans des domaines spécifiques de la SRI (par ex. sensibilisation). L'Agence s'appuiera sur ses contacts et réseaux existants, y compris les agents de liaison nationaux et les organes nationaux compétents.
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.)
Objectif SMART: D'ici à 2010, au moins 10 États membres ont participé à au moins 3 modèles différents de coopération. **ICP:** # d'États membres participants, # de modèles de coopération
OBJECTIFS SUPÉRIEURS APPUYÉS PAR LE PROGRAMME
Développer la confiance dans la société de l'information en renforçant les capacités des États membres en matière de SRI.
Accroître la coopération entre les États membres afin de réduire leurs différences de capacités dans ce domaine. Renforcer le dialogue sur la SRI entre les diverses parties prenantes en Europe.
PARTIES PRENANTES + BÉNÉFICIAIRES
Gouvernements d'États membres (et ARN), Commission, industrie, universités, autres groupes de parties prenantes.
POURQUOI L'ENISA?
L'ENISA détient une position unique pour prêter conseil et assistance aux États membres et à la Commission en vue du renforcement de leurs capacités en matière de sécurité des réseaux et de l'information. L'ENISA fournit une plate-forme indépendante à toute l'Europe pour faciliter la coopération entre les États membres, en agissant en tant que tiers de confiance. L'ENISA a déjà accompli un précieux travail dans différents domaines tels que sensibilisation, CSIRT, étude de faisabilité sur un système d'échange d'information et d'alerte à l'échelle européenne et fonction d'intermédiaire entre les États membres et les micro-entreprises.
PROGRAMME PROPOSÉ PAR:
ENIDA, conseil d'administration, groupe permanent des parties prenantes
BASE JURIDIQUE
Règlement ENISA, article 3, points c), d) et e)

2.2.1 L.T. 2.1 – Plate-forme de coopération pour la communauté de sensibilisation

Nom du PTPA:	
Développer et entretenir des modèles de coopération	
NOM DU LOT DE TRAVAUX:	
L.T. 2.1: Plate-forme de coopération pour la communauté de sensibilisation	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: D'ici au 4e trimestre 2010, disposer d'au moins cinq livres blancs rédigés avec le soutien de la communauté de sensibilisation. Les thèmes seront identifiés en prenant en considération la composition de la communauté de sensibilisation (par ex. les intérêts des membres) et des recherches/études menées par l'Agence.	**ICP:** # de livres blancs
Objectif SMART: D'ici au 2e trimestre 2010, organiser une conférence réunissant au moins 100 participants d'au moins 10 États membres de l'UE.	**ICP:** # de participants, # d'États membres de l'UE représentés
DESCRIPTION DU LOT DE TRAVAUX	
Ce lot de travaux est destiné à poursuivre le développement et à renforcer la communauté de sensibilisation, ainsi qu'à maintenir son statut de plate-forme efficace de coopération pour la sensibilisation aux questions de sécurité et la promotion des bonnes pratiques de SRI dans toute l'UE. Il est également prévu de demander à la communauté de sensibilisation de soutenir l'ENISA dans sa mission de promotion d'une culture de la sécurité de l'information. À cet effet, deux volets principaux ont été identifiés pour permettre d'atteindre ces buts: la communauté de sensibilisation et la conférence de sensibilisation. **La communauté de sensibilisation** L'ENISA poursuivra le développement et le renforcement de la communauté de sensibilisation, qui vient de connaître deux ans de croissance rapide. L'Agence facilitera les discussions, l'échange de bonnes pratiques et le partage de connaissances par différents moyens de communication durant lesquels seront abordés et examinés des sujets d'actualité, des questions clés et des bonnes pratiques de sensibilisation émergentes. Les membres de la communauté de sensibilisation seront invités à collaborer avec la section Sensibilisation de l'ENISA à la réalisation de sa mission de favoriser une culture de la sécurité de l'information. Les membres constitueront un point de contact pour les questions concernant la sensibilisation à la sécurité de l'information en général ou portant spécifiquement sur leur pays, leur secteur ou leur domaine d'activité. Ils feront une contribution par exemple en participant à des débats et à la rédaction de livres blancs sur des thèmes de sécurité spécifiques, notamment la sensibilisation des PME, mais aussi en prenant part à des groupes de travail virtuels et en poursuivant les tâches actuelles. Les documents nécessaires seront disponibles sur le portail de la communauté de sensibilisation (par ex. des rapports, des moyens de formation et des fiches d'information). **La conférence de sensibilisation** Au deuxième trimestre 2010, l'ENISA organisera une conférence afin de présenter les bonnes pratiques de sensibilisation actuelles. Les sujets seront sélectionnés sur la base des conclusions tirées par l'ENISA et la communauté de sensibilisation dans le domaine de la sensibilisation à la sécurité de l'information.	
RÉSULTATS ET CALENDRIER:	
Conférence de sensibilisation dont le but est de présenter des documents de bonnes pratiques et des recommandations pour améliorer la coopération entre États membres (2e trimestre 2010) Liste et coordonnées des experts en sensibilisation faisant partie de la communauté de sensibilisation de l'ENISA (tâche en cours; 4e trimestre 2010)	
PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:	
États membres, groupe permanent des parties prenantes, associations sectorielles, communauté de sensibilisation	
RESSOURCES POUR 2010 (personnes-mois et budget)	

• 24 personnes-mois • 60 000 euros
LOT DE TRAVAUX PROPOSÉ PAR:
ENISA
BASE JURIDIQUE
Règlement ENISA, article 3, points c), d) et e)

2.2.2 L.T. 2.2 – Cercle de compétence en matière de sécurité et partage de bonnes pratiques pour les communautés CERT

Nom du PTPA:	
Développer et entretenir des modèles de coopération	
NOM DU LOT DE TRAVAUX:	
L.T. 2.2: Cercle de compétence en matière de sécurité et partage de bonnes pratiques pour les communautés CERT	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: D'ici au 4e trimestre 2010, au moins 10 références aux documents de l'ENISA sur les bonnes pratiques «services CERT» faites par des sites internet externes, des publications officielles, des débats, des listes de diffusion ou autres moyens.	**ICP:** # de références
Objectif SMART: D'ici au 4e trimestre 2010, au moins 10 références aux documents de l'ENISA soutenant la coopération paneuropéenne entre CERT nationaux ou gouvernementaux, faites par des sites internet externes, des publications officielles, des débats, des listes de diffusion ou autres moyens.	**ICP:** # de références
Objectif SMART: Au moins 50 % de la population de l'UE est représentée à l'atelier sur les CERT	**ICP:** % de la population de l'UE représentée
Objectif SMART: Les participants à l'atelier sur les CERT lui donnent une note d'au moins 3 sur une échelle de 1 à 5	**ICP:** Moyenne du retour d'informations sur une échelle de 1 à 5
Objectif SMART: D'ici au 4e trimestre 2010, au moins 3 exposés présentés concernant l'action de l'ENISA dans le domaine CERT à des manifestations des communautés CERT/CSIRT.	**ICP:** # d'exposés
Objectif SMART: D'ici au 4e trimestre 2010, 80 % des mises à jour de répertoires de CERT sont confirmées	**ICP:** % de mises à jour confirmées
Objectif SMART: D'ici au 4e trimestre 2010, au moins deux formations TRANSISTS ont été organisées avec le soutien de l'ENISA[8]	**ICP:** # de formations soutenues
DESCRIPTION DES TÂCHES:	
Les travaux de l'ENISA dans le domaine de la coopération et du soutien des CERT ont atteint un point crucial: presque tous les États membres de l'UE ont mis en place au moins une équipe d'intervention pouvant agir comme point de contact intermédiaire pour le signalement et la gestion des incidents, ou ont lancé des projets qui déboucheront sur l'établissement d'une équipe de ce type. Toutefois, certains États membres n'ont pas encore mis en place un CERT national ou gouvernemental doté d'un mandat officiel pour fournir des services de protection des infrastructures nationales d'information et coopérer avec les CERT nationaux ou gouvernementaux d'autres États membres. Par conséquent, cette année, l'ENISA s'efforcera de faciliter encore l'établissement, la formation et l'exercice des capacités nationales ou gouvernementales en matière de CERT ainsi que leur coopération au niveau européen. Dans le cadre d'efforts spéciaux pour favoriser la coopération entre les CERT nationaux ou gouvernementaux, des débats seront tenus avec les parties prenantes et un consensus sera recherché concernant les capacités, exigences, besoins, obstacles et autres questions, en vue de permettre à tous les États membres de participer aux activités de partage des informations sur les incidents, les vulnérabilités et autres thèmes liés à la PIIC. **Bonnes pratiques de fourniture de services CERT** Sur la base de l'enquête de 2009 ayant débouché sur l'élaboration d'une liste de «capacités minimales pour les CERT nationaux ou gouvernementaux en Europe», une analyse plus approfondie des bonnes pratiques	

[8] À condition que l'organisateur des stages TRANSITS réguliers poursuive cet effort.

de fourniture de ces services sera réalisée. L'ENISA élaborera un guide de bonnes pratiques concernant un service spécifique qui est décrit comme important dans cette liste et qui n'est pas encore repris dans un recueil de bonnes pratiques. Les services les plus prometteurs pourraient être les suivants:

- Surveillance et avertissement précoce (et thèmes liés tels que la détection d'anomalie, la corrélation d'évaluation, les réseaux de capteurs, etc.).
- *Recherche et divulgation des vulnérabilités.*
- *Anal*yse des logiciels malveillants (et thèmes liés comme les honeypots, honeynets, malware-db, etc.).

Faciliter la coopération et le partage d'informations
La coopération et le partage des informations à l'échelon européen entre les CERT nationaux ou gouvernementaux revêt une importance cruciale pour une approche paneuropéenne de la gestion des incidents. L'ENISA déterminera comment assister la communauté des CERT pour faciliter la coopération et le partage d'informations en son sein. Elle prendra comme point de départ un document de référence pour soutenir la coopération paneuropéenne entre les CERT nationaux ou gouvernementaux, basé sur le rapport «coopération entre les CERT et sa facilitation par les parties prenantes concernées» (2006). L'ENISA actualisera ce rapport en mettant l'accent sur les besoins organisationnels des États membres en ce qui concerne le partage d'informations. Des expériences d'initiatives telles que le Groupe des CERT gouvernementaux européens (EGC) ou les ISAC sectoriels alimenteront ce document. De plus, celui-ci renseignera l'ENISA sur les prochaines étapes cruciales en vue des prochaines années. L'élaboration de ce nouveau document ira de pair avec un débat par les parties prenantes concernées, qui prendra des formes appropriées comme des groupes de travail *ad hoc*, des exposés lors de réunions de CERT, etc.

Renforcer les capacités des États membres – suivi du SEPIA
En 2006/2007, l'ENISA a réalisé une étude pour évaluer la «Faisabilité d'un système européen d'échange d'information et d'alerte» (SEPIA), destiné aux PME et aux citoyens. En 2009/2010, deux projets pilotes complémentaires visant à mettre en œuvre les conclusions de cette étude sont menés avec le soutien financier de la Commission européenne. Dans sa communication COM(2009(149)), la Commission européenne invite l'ENISA à faire l'inventaire, pour fin 2010, des résultats de ces deux projets et d'autres initiatives nationales et à établir une feuille de route afin de promouvoir le développement et le déploiement du SEPIA. En 2009, l'ENISA a commencé à suivre le processus de réalisation de ces deux projets et, en fonction de la disponibilité des chefs de projet, continuer à en suivre les progrès en 2010. L'ENISA vise à élaborer le projet de feuille de route pour fin 2010 en tenant compte des résultats des projets et d'autres initiatives (nationales). La feuille de route est censée indiquer la voie à suivre pour la poursuite du développement dans le domaine du partage d'informations pour les citoyens et les PME.

5^{e} atelier de l'ENISA sur le thème «CERTs in Europe»
L'ENISA favorisera le dialogue avec les parties prenantes en proposant un atelier aux acteurs clés des États membres et de la Commission européenne. La 5^{e} édition de l'atelier «CERTs in Europe» se focalisera sur «le rôle des CERT nationaux ou gouvernementaux dans les exercices nationaux et internationaux» et visera à partager les informations sur les bonnes pratiques méthodologiques et organisationnelles pour les CERT nationaux ou gouvernementaux qui participent à des exercices de PIIC dans leur État membre. En outre, cet atelier abordera le thème de la participation aux exercices internationaux tels qu'ASEAN Drill, Cyberstorm, etc. Les résultats de l'atelier serviront à définir les mesures suivantes que l'ENISA peut prendre avec les parties prenantes concernées afin de renforcer les capacités des CERT nationaux ou gouvernementaux en matière d'exercices internationaux; ces résultats seront également utilisés pour faciliter l'esquisse du cadre d'exercices décrit dans la section PTPA 1 «Résilience» du L.T. 1.4.

Poursuivre la facilitation de la mise en place de CERT/CSIRT et rester en relations étroites avec les diverses communautés CERT/CSIRT
L'ENISA a élaboré et continuera d'élaborer des outils (comme les guides de création et de gestion d'un CSIRT, le guide de la coopération et le recueil d'exercices pour les CSIRT) pour le renforcement de la communauté CERT et de sa coopération, et s'efforce d'apporter une aide pour la création de nouveaux

CERT gouvernementaux ou nationaux dans les États membres. À cette fin, le soutien des très précieuses formations TRANSITS organisées deux fois par an en Europe pour les membres du personnel des CSIRT sera maintenu. Il sera peut-être possible de répondre aux demandes des États membres concernant des formations spéciales pour le personnel des CERT, comme cela s'est produit par le passé, pour remédier aux failles des services CERT en Europe, en particulier concernant la couverture gouvernementale/nationale des CERT. Le répertoire des CERT de l'ENISA sera actualisé pour refléter les changements survenus dans le paysage européen.

Présenter et représenter

L'ENISA continuera en outre à renforcer sa position de point de contact indépendant et expérimenté pour les diverses communautés CERT européennes et internationales comme TF-CSIRT et FIRST. Cela sera accompli en présentant l'action de l'ENISA à des manifestations organisées par ces communautés et en permettant aux communautés d'influencer l'action de l'Agence par des informations en retour.

RÉSULTATS ET CALENDRIER:

- Guide de bonnes pratiques de l'ENISA sur la prestation d'un service CERT (4e trimestre)
- Document de référence de l'ENISA sur la coopération entre CERT nationaux ou gouvernementaux à l'échelle européenne (4e trimestre)
- Projet de feuille de route «SEPIA» au 4e trimestre 2010
- 5e atelier «CERTs in Europe» (2e trimestre)
- Mise à jour de l'«ENISA Inventory of CERTs in Europe» (Inventaire des CERT par l'ENISA en Europe) aux 2e et 4e trimestres 2010
- Au moins 2 stages TRANSITS soutenus au 4e trimestre

PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:

États membres de l'UE (en particulier CSIRT nationaux), Commission européenne, communauté CERT

RESSOURCES POUR 2009 (personnes-mois et budget)

- 135 000 euros (ateliers, réunions, expertise conseil, facilitation d'exercice, soutien des stages TRANSITS)
- 24 personnes-mois

LOT DE TRAVAUX PROPOSÉ PAR:

ENISA, Commission européenne

BASE JURIDIQUE

Règlement ENISA, article 3, points c), d) et e)

2.2.3 L.T. 2.3 – Facilitation de l'échange de bonnes pratiques de SRI au niveau européen

PTPA	
Développer et entretenir des modèles de coopération	
NOM DU LOT DE TRAVAUX:	
L.T. 2.3: Facilitation de l'échange de bonnes pratiques de SRI au niveau européen	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: D'ici au 3e trimestre 2010, publication des rapports pays et du répertoire Who-is-Who couvrant les politiques de SRI, les pratiques de gouvernance et les contacts en résilience des IIC, l'identité électronique et la notification des atteintes aux données à caractère personnel dans tous les États membres (y compris les pays de l'EEE et de l'AELE).	**ICP:** # de bonnes pratiques identifiées en matière de résilience des IIC, d'identité électronique et de notification des atteintes
Objectif SMART: D'ici au 4e trimestre 2010, lancement de projets d'échange de bonnes pratiques en matière de résilience des IIC, d'identité électronique et de notification des atteintes pour les pays en besoin critique, comme identifiés dans les rapports pays.	**ICP:** # de parties prenantes et # de pays participant à des projets en matière de résilience des IIC, d'identité électronique et de notification des atteintes, par rapport aux besoins identifiés dans les rapports pays.
DESCRIPTION DES TÂCHES:	

Depuis 2007, l'ENISA facilite les projets de coopération entre États membres de l'UE par le biais de son initiative de facilitation de l'échange de bonnes pratiques de SRI au niveau européen.

Les activités d'échange déjà réalisées sont notamment:

- Dans le domaine des CERT, l'ENISA a facilité des projets de coopération entre la Hongrie et la Bulgarie afin d'établir le CERT gouvernemental bulgare, et entre le CERT-FI (Finlande) et le CSIR/MERAKA (Afrique du Sud) afin d'échanger de bonnes pratiques et de mettre en place un CSIRT sud-africain.
- Dans le *secteur financier*, l'ENISA a facilité le développement d'un partenariat public-privé pour l'échange structuré d'informations liées à la cybercriminalité entre le secteur financier et les gouvernements, au moyen de Centres d'information et d'analyses financières (FI-ISAC) impliquant plus de 15 pays et les parties prenantes concernées du secteur privé.
- Dans le domaine de la *sensibilisation*, en 2009, l'ENISA a facilité une réunion de gouvernements locaux scandinaves visant à mettre en place des échanges de bonnes pratiques concernant la gestion des informations de sécurité dans des municipalités et région du Danemark, de Suède et de Norvège.
- Dans le domaine de *la résilience et des CERT*, l'ENISA compte faciliter un projet de coopération entre Malte et un (ou plusieurs) autre(s) pays vers la fin 2009 ou le début 2010.

Pour renforcer le niveau global de SRI en Europe, il est impératif de beaucoup améliorer la coopération entre les États membres et le secteur privé. La communication de la Commission européenne de 2009 intitulée «Protéger l'Europe des cyberattaques et des perturbations de grande envergure: améliorer l'état de préparation, la sécurité et la résilience» appelle à la mise en place d'un nouveau modèle multipartite d'envergure européenne favorisant «l'engagement du secteur privé dans la définition d'objectifs stratégiques de politique publique [...]» (cf. point 3.4.2). S'appuyant sur ses premières réussites avec le secteur financier, l'ENISA continuera à développer ses activités de partage non seulement avec les États membres (y compris les pays de l'EEE) et les pays tiers mais aussi avec de grandes organisations des secteurs public et privé. Ce projet permettra:

1. Le transfert de bonnes pratiques entre les pays disposant déjà de structures développées et ceux qui n'en ont pas.
2. L'identification et l'élaboration des nouvelles pratiques de gouvernance dont certains pays – si pas tous – ont besoin en raison des menaces émergentes.

En 2010, le lot de travaux sur l'échange de bonnes pratiques sera davantage intégré aux travaux en cours au niveau du PTPA 1 et de l'AP 1. Les projets de coopération vont donc se centrer sur le développement de l'échange de bonnes pratiques en matière d'*infrastructures et services résilients, durables et sûrs*, l'amélioration des *équipes nationales ou gouvernementales d'intervention en cas d'urgence informatique (CERT) et le développement de forums de coopération publics-privés tels que le SEPIA et le FI-ISAC*, et les questions *d'identité électronique, d'authentification, de protection des données, de vie privée et de confiance*, cela dans le but d'identifier les mesures clés permettant de maintenir un degré élevé de sécurité et de confiance dans un certain nombre de secteurs à évolution très rapide qui revêtent une importance vitale pour les États membres.

Afin d'identifier les bonnes pratiques et les partenaires potentiels des projets de coopération à mener dans ces domaines cruciaux, tout en se basant sur le savoir-faire déjà acquis, l'Agence recentrera les rapports pays existants sur les politiques et les pratiques de gouvernance relatives à la résilience des IIC, à l'authentification et à la gestion des données à caractère personnel (en particulier les notifications d'atteintes). Ces rapports fourniront ainsi un inventaire des bonnes pratiques en matière de SRI et seront complétés par un répertoire Who-is-Who, également recentré, qui identifiera les parties prenantes – tant publiques que privées – concernées par ces domaines.

L'échange de bonnes pratiques en matière de SRI sera soutenu par une plate-forme en ligne (un extranet destiné aux parties prenantes que l'ENISA compte mettre en place à partir de septembre 2009) proposant des informations sur les projets de coopération achevés ou en cours, un inventaire des bonnes pratiques de SRI ainsi que la publication en ligne des rapports pays et du répertoire Who-is-Who. Cette plate-forme en ligne servira donc de source d'information sur les bonnes pratiques en matière de SRI et d'outil pour identifier et contacter les partenaires potentiels de projets de coopération.

RÉSULTATS ET CALENDRIER

Projets en coopération (4e trimestre 2010)
Rapports pays et répertoire Who-is-Who (3e trimestre 2010)
Plate-forme en ligne (en cours, 2e trimestre 2010)

PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:

États membres: conseil d'administration, agents de liaison nationaux, groupe permanent des parties prenantes; réseaux de diverses «communautés sectorielles» (secteur privé: industrie, utilisateurs/consommateurs, universités, etc.).

RESSOURCES POUR 2010 (personnes-mois et budget)

- 120 000 euros
- 7 personnes-mois

LOT DE TRAVAUX PROPOSÉ PAR:

ENISA

BASE JURIDIQUE

Règlement ENISA, article 3, points c) et d)

2.3. PTPA 3: Identifier les risques émergents afin d'instaurer la confiance

NOM DU PROGRAMME
Identifier les risques émergents afin d'instaurer la confiance
DESCRIPTION DU PROBLÈME À RÉSOUDRE
Les décideurs des secteurs public et privé ont besoin de se faire une idée claire de la nature et de l'impact des défis émergents et futurs que peut poser la sécurité informatique dans notre société de l'information. Ces défis sont liés aux risques de sécurité inhérents aux applications et technologies émergentes et futures qui font leur apparition sur le marché européen. Une connaissance accrue des risques émergents et futurs pourrait permettre aux parties prenantes des secteurs public et privé de prendre des décisions plus avisées et de disposer d'une meilleure base pour l'élaboration des politiques. En 2010, l'ENISA produira des rapports d'évaluation des risques émergents et futurs pour des scénarios spécifiques d'applications et de technologies. Ces scénarios reflèteront les avis des diverses parties prenantes de l'Europe mais prendront également en compte les autres activités de l'ENISA relatives à l'identification des risques émergents en tant que question transversale (par ex.: l'AP 1).
DESCRIPTION DE L'APPROCHE RETENUE POUR RÉSOUDRE LE PROBLÈME:
En 2008-2009, l'Agence a établi un cadre destiné à permettre aux parties prenantes de mieux identifier et comprendre les risques émergents et futurs liés aux nouvelles technologies et aux nouvelles applications, un travail intitulé *Cadre des risques émergents et futurs*. En 2008 et 2009, l'ENISA a constitué des groupes d'experts afin de valider et analyser les scénarios soumis selon une perspective axée sur les risques. Le forum des parties prenantes de l'ENISA a joué un rôle prépondérant dans les activités de l'ENISA relatives aux risques émergents et futurs; en effet, ce forum nous a apporté des conseils judicieux et des informations en retour précieuses pour l'orientation de nos activités. En 2010, le forum des parties prenantes sur les risques émergents et futurs continuera, et son travail sera complété par des groupes d'experts spécialisés qui contribueront à l'analyse et l'identification de ces risques grâce à leur savoir-faire spécialisé (par ex. groupes d'experts virtuels et experts spécialisés). Les travaux de ces deux groupes seront partagés avec d'autres activités de l'ENISA dans le cadre du programme de travail 2010 (en particulier l'AP 1). Par son utilisation du cadre des risques émergents et futurs, l'Agence soutiendra le programme de travail en élaborant des rapports d'évaluation des risques concernant les scénarios de domaines liés au PTPA 1 et à l'AP 1. Les travaux de l'ENISA sur les risques émergents et futurs ont pour but de promouvoir une approche proactive des défis émergents et futurs découlant des technologies et applications nouvelles ou émergentes. Cette activité vise à stimuler la confiance dans la société de l'information, en particulier dans d'importants domaines tels que la résilience, l'identité et la confiance. À ce titre, les risques émergents et futurs deviennent une fonction de soutien transversal pour d'autres PTPA de l'ENISA dans leurs aspects d'identification des risques émergents. Dans le cadre de ce PTPA, l'ENISA définira un processus d'identification des thèmes ou scénarios de candidats à analyser (c.-à-d. une carte conceptuelle pour la sélection des thèmes, la sélection des scénarios et la communication). Ce processus aidera l'ENISA à sélectionner les scénarios à analyser, et à déterminer dans quels domaines thématiques ils doivent être analysés. En appui aux activités de la Commission dans le domaine de la PIIC, et en particulier en vue des exercices à mener au niveau paneuropéen, l'ENISA réalisera une évaluation initiale des éléments pertinents pour l'état de préparation à la gestion des risques au niveau national. Ce travail permettra d'établir une liste de domaines et d'aspects considérés comme les composantes d'un portefeuille de l'état de préparation à la gestion des risques au niveau national. Par la suite, les composantes ou domaines susceptibles de faire partie d'un exercice paneuropéen seront identifiés (selon leur profil de risque). Sur cette base, divers scénarios d'exercice pourront être mis au point. Cette activité sera menée à bien par un groupe d'experts européens dans ce domaine (groupe de travail) et coordonnée dans le cadre des activités du L.T. 1.4.

Enfin, il importe de noter que, au sein de ce PTPA, il sera tenu compte d'initiatives similaires appartenant au domaine des menaces ou risques émergents et futurs mais aussi à celui de la PIIC. Des interfaces avec les programmes et activités de recherche correspondants de la Commission européenne ayant été établies, l'ENISA restera en contact étroit avec cette institution afin d'identifier toutes les initiatives pertinentes (par ex. l'interaction avec les États membres concernant les prochaines recommandations relatives à la RFID).

OBJECTIFS SUPÉRIEURS APPUYÉS PAR LE PROGRAMME

Faciliter le marché intérieur des communications électroniques en aidant les parties prenantes européennes à choisir le dosage approprié de mesures, c'est-à-dire techniques ou organisationnelles et juridiques (en soulignant en particulier l'importante contribution que peut apporter l'Agence à la directive-cadre).
Renforcer le dialogue sur la SRI entre les diverses parties prenantes dans l'UE.
Développer la confiance dans la société de l'information en relevant le niveau de la SRI dans l'UE.

IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.)

Objectif SMART: D'ici à 2010, au moins 20 parties prenantes ou organisations participantes d'au moins 10 États membres nomment l'ENISA comme point de référence pour discuter de la nature et de l'impact des défis émergents pour la sécurité informatique dans la société de l'information.

ICP: # de parties prenantes, # d'États membres

PARTIES PRENANTES + BÉNÉFICIAIRES

Décideurs des secteurs public et privé, tels que gouvernements d'États membres, industries, organisations de R&D, développeurs de logiciels, intégrateurs de systèmes et organismes de normalisation qui soumettront des scénarios émergents à analyser.

POURQUOI L'ENISA?

L'ENISA possède la capacité requise pour réunir les parties prenantes pertinentes afin de faciliter la discussion et l'échange d'informations au niveau européen.

L'ENISA a effectué en 2006 et 2007 une évaluation des risques pour la sécurité de l'information liés aux applications émergentes. Elle a également mis en œuvre une feuille de route et exécuté des études sur les mécanismes pour la collecte, le traitement et la diffusion des informations sur les risques émergents. Elle a par ailleurs publié plusieurs documents de synthèse sur les tendances technologiques et les risques concernant les domaines émergents, et mis en place les groupes consultatifs nécessaires (formés d'experts).

L'ENISA a établi un Forum des parties prenantes destiné à jouer un rôle directeur dans l'évaluation et l'analyse des risques émergents et futurs, et maintient une équipe d'experts pour l'évaluation des risques des scénarios applicatifs et technologiques émergents.

L'ENISA contribue au domaine de la PIIC et peut apporter des éléments précieux pour les exercices paneuropéens.

PROGRAMME PROPOSÉ PAR:

ENIDA, conseil d'administration, groupe permanent des parties prenantes

BASE JURIDIQUE

Règlement ENISA, article 3, points a), c), d) ,e), f), g), i) et k)

2.3.1 L.T. 3.1 – Cadre pour l'évaluation et la discussion des risques émergents – Analyse de scénarios spécifiques

Nom du PTPA:	
Identifier les risques émergents afin d'instaurer la confiance	
NOM DU LOT DE TRAVAUX:	
L.T. 3.1: Cadre pour l'évaluation et la discussion des risques émergents – Analyse de scénarios spécifiques	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: D'ici au 4e trimestre 2010, atteindre un taux de satisfaction au-dessus de la moyenne (3 sur une échelle de 1 à 5; 1 = bas, 5 = max.) parmi les parties prenantes participant à l'analyse des scénarios de risques émergents et futurs.	**ICP:** taux de satisfaction (1-5, 1 = bas, 5 = max.)
Objectif SMART: D'ici au 4e trimestre 2010, au moins deux scénarios analysés.	**ICP:** # de scénarios analysés, et qualité des évaluations
Objectif SMART: D'ici au 4e trimestre 2010, au moins 6 références à des documents publiés concernant les scénarios analysés.	**ICP:** # de références
DESCRIPTION DES TÂCHES:	
Ce L.T. a pour objectif d'identifier les risques émergents et futurs pour certains domaines de technologies et d'applications, sur la base du cadre des risques émergents et futurs qui a été élaboré et validé lors du programme de travail précédent (2008 et 2009). Dans ce contexte, plusieurs évaluations seront réalisées afin d'identifier les risques émergents et futurs des scénarios applicatifs et technologiques (les *scénarios*). Au moins deux scénarios seront sélectionnés selon les indications de nos parties prenantes (c.-à-d. les parties prenantes ou organisations soumettant une demande à analyser au regard du cadre des risques émergents et futurs de l'ENISA, par exemple par le forum des parties prenantes, le groupe permanent des parties prenantes ou les groupes d'experts virtuels). Les scénarios à analyser seront examinés de la même façon qu'en 2009 et leur degré de priorité sera fixé par les comités de l'ENISA (par ex. le forum des parties prenantes sur les risques émergents et futurs, le groupe permanent des parties prenantes et le conseil d'administration de l'ENISA). En particulier, les évaluations permettront d'identifier les risques émergents et futurs dans les domaines de la résilience des infrastructures d'information et de la vie privée. Dans le but de maximiser les synergies et de produire un impact plus fort, l'élaboration du scénario de résilience s'effectuera sur la base des travaux menés au sein du PTPA 1. De même, les travaux de la Commission dans ce domaine, en particulier sa récente recommandation sur la RFID (http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf), seront utilisés pour alimenter le scénario sur la vie privée. Pendant l'analyse des scénarios, des questions politiques seront examinées, notamment les préoccupations relatives à la vie privée et d'autres questions sociales. À cet effet, des jalons seront définis pendant les phases d'analyse, ce qui permettra de prendre des décisions sur le type d'élaboration (en profondeur, groupes cibles de parties prenantes et qualité) à adopter pour les questions politiques. Les activités concernées de la Commission européenne ou d'autres décideurs seront prises en compte. De plus, ces travaux seront coordonnés avec les travaux d'analyse de scénarios réalisés dans le cadre d'autres lots de travaux (l'AP 1.1). Chaque analyse de scénario sera conduite avec le soutien d'experts. À cet effet, il sera fait usage des listes de réserve d'experts établies en 2009; on s'attend évidemment à ce que de nouveaux experts se proposent et soient inclus dans ces listes de réserve. Une partie du budget servira à rémunérer les experts participants. Le forum des parties prenantes sur les risques émergents et futurs contribuera à ce LT en lui offrant des informations en retour et en supervisant les résultats des travaux (assurance qualité des scénarios analysés, examen, commentaires sur l'approche d'évaluation).	

Dans ce LT, l'ENISA examinera et contactera les activités existantes ou similaires menées au niveau européen afin de leur offrir des contributions ou conseils et d'éviter toute duplication du travail. Les représentants concernés des DG de la Commission européenne peuvent devenir membres observateurs du forum des parties prenantes de l'ENISA sur les risques émergents et futurs et faire la liaison entre l'ENISA et ces DG sur divers sujets tout en apportant des contributions à nos travaux.

L'ENISA a déjà établi des contacts étroits, qu'elle poursuivra, avec des activités et actions de coordination semblables financées par le 7e programme-cadre de la Commission européenne, telles que FORWARD et WOMBAT. Les échanges d'informations avec d'autres parties prenantes de l'UE, comme la DG ESTAT, seront également maintenus. Outre les activités de la Commission européenne, d'autres initiatives appropriées peuvent être communiquées par des experts externes et/ou des membres du groupe permanent des parties prenantes que nous envisageons de consulter au cours de la mise en œuvre de notre programme de travail. À cet effet, un canal de communication permanent sera établi avec les experts.

RÉSULTATS ET CALENDRIER:

Au moins deux évaluations des risques de scénarios sélectionnés (3e et 4e trimestres 2010) sous la forme de rapports d'évaluation des risques
Présentation des outils élaborés à l'occasion d'événements dans le domaine de la sécurité
Gestion du forum des parties prenantes et de la réserve d'experts

PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:

Forum des parties prenantes sur les risques émergents et futurs de l'ENISA, industrie, universités, organismes de normalisation, membres du groupe permanent des parties prenantes

RESSOURCES POUR 2010 (personnes-mois et budget)

- 120 000 euros
- 16 personnes-mois

LOT DE TRAVAUX PROPOSÉ PAR:

ENISA

BASE JURIDIQUE

Règlement ENISA, article 3, points a), c), d), e), f), g), i) et k)

2.3.2 L.T. 3.2 – Maintenance du cadre des risques émergents et futurs

Nom du PTPA:	
Identifier les risques émergents afin d'instaurer la confiance	
NOM DU LOT DE TRAVAUX:	
L.T. 3.2 – Maintenance du cadre des risques émergents et futurs	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: D'ici à 2011, au moins deux références dans des publications pertinentes et au moins une présentation du modèle prédictif à l'occasion d'un événement pertinent	**ICP:** # de références, # de présentations dans des événements pertinents, # date
Objectif SMART: D'ici à 2011, au moins deux parties prenantes désireuses d'adopter la fonctionnalité mise au point	**ICP:** # de parties prenantes participant au groupe de travail
DESCRIPTION DU LOT DE TRAVAUX	
L'objectif de ce lot de travaux est d'améliorer les fonctions du cadre des risques émergents et futurs. Des capacités additionnelles relatives à la gestion et la diffusion des informations recueillies seront élaborées, ainsi que des interfaces avec d'autres sources concernées (incidents, menaces et vulnérabilités, etc.). Ce contenu du lot de travaux sera développé sur les conseils d'un groupe d'experts qui prendra la forme d'un groupe de travail ad hoc (groupe de travail sur les risques émergents et futurs). Le principal livrable de ce lot de travaux sera une ***carte conceptuelle pour la sélection des scénarios et la maintenance du cadre des risques émergents et futurs***. Le cadre des risques émergents et futurs étant un processus dynamique, nous comptons utiliser les retours d'information que nous recevons concernant son application dans le LT 3.1 ainsi que des travaux précédents du programme de travail 2009, cela afin de mettre le cadre à jour et d'en améliorer le fonctionnement. Un élément particulièrement important sera la mise à jour du processus d'identification et de sélection des domaines et scénarios appropriés (technologies et applications) qui démarre l'ensemble du processus; cette mise à jour se justifie par la nécessité d'avoir, comme base de la sélection, un modèle conceptuel facilitant l'identification et la sélection d'un scénario en plus du domaine approprié (approches axées sur les technologies par rapport aux autres approches telles que la politique, les thèmes sociétaux, etc.). Cet élément est essentiel car l'identification d'un scénario correct est critique pour la réalisation d'un impact et, partant de là, est un important facteur de réussite pour ces travaux. Ce résultat contribuera à l'identification rapide, transparente et systématique des domaines thématiques et des scénarios.	
RÉSULTATS ET CALENDRIER:	
• Un modèle conceptuel et un processus de sélection des domaines thématiques et des scénarios (d'ici au 1er trimestre 2010), y compris un système de pondération et d'établissement des priorités.	
PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:	
Conseil d'administration, groupe permanent des parties prenantes, ALN, membres du groupe de travail (industrie, universités, recherche), forum des parties prenantes sur les risques émergents et futurs	
RESSOURCES POUR 2010 (personnes-mois et budget)	
• 35 000 euros • 3 personnes-mois	
LOT DE TRAVAUX PROPOSÉ PAR:	
ENISA	
BASE JURIDIQUE	
Règlement ENISA, article 3, points a), c), d),e), f), g), i) et k)	

2.3.3 L.T. 3.3 – Renforcement de la préparation en matière de gestion nationale des risques

Nom du PTPA:	
Identifier les risques émergents afin d'instaurer la confiance	
NOM DU LOT DE TRAVAUX:	
L.T. 3.3 – Renforcement de la préparation en matière de gestion nationale des risques: mesure d'appui à l'exercice paneuropéen	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: identification d'experts européens dans le domaine de la préparation en matière de gestion nationale des risques	**ICP: #** d'experts participant au groupe de travail
Objectif SMART: D'ici à la fin 2010, une liste des principaux domaines à considérer comme faisant partie de la préparation en matière de gestion nationale des risques en vue de la PIIC sera établie. À partir de ce document, une liste des domaines/composantes liés à la PIIC sera établie et documentée (critère: aspects relatifs aux risques). Les scénarios de l'exercice en seront inspirés.	**ICP:** caractère complet de la liste et inclusion de thèmes concernés par la préparation en matière de gestion nationale des risques. Les scénarios de l'exercice seront élaborés sur la base des domaines/composantes identifiés.
Objectif SMART: D'ici la fin 2010, au moins deux États membres sont intéressés par les résultats et désirent faire de même.	**ICP:** # d'États membres intéressés
DESCRIPTION DU LOT DE TRAVAUX	
La PIIC et la résilience des réseaux de communication forment un domaine qui concerne beaucoup de parties prenantes et de secteurs, de la technologie à la politique en passant par la coopération et la communication entre organisations. La gestion proactive des risques liés à l'information est une question clé pour la construction et le maintien d'infrastructures d'information résilientes. Quand on examine les éléments des risques liés aux biens d'information (tant techniques qu'organisationnels), il importe de prendre en compte différents aspects qui varient en fonction de la nature, de l'importance et de l'impact propres à ces informations dans le contexte de la PIIC. De plus, considéré au niveau d'un État membre, l'établissement ou le renforcement de l'état de préparation en matière de gestion nationale des risques doit associer de multiples parties prenantes des secteurs privé et public. Avec ce lot de travaux, nous cherchons à effectuer une identification initiale des domaines pouvant être considérés comme nécessaires pour la préparation en matière de gestion nationale des risques, ainsi que l'identification des parties prenantes concernées dans les États membres de l'UE. Les questions liées à la PIIC seront le principal élément à employer pour identifier ces domaines, mais d'autres domaines ayant un lien direct avec la PIIC entreront également en considération. L'accent sera mis sur les liens importants existant entre ces domaines et les principales composantes envisagées. Le résultat final sera un premier tableau des domaines et composantes, avec l'indication des parties prenantes et de leurs rôles dans la préparation en matière de gestion nationale des risques. Ce résultat s'atteindra en constituant un groupe de travail d'experts nationaux dans le domaine de la gestion des risques, avec la participation d'organisations publiques et privées. Ce groupe de travail aura pour tâche d'identifier et de décrire tous les éléments pertinents de la préparation en matière de gestion nationale des risques au regard de la résilience des réseaux publics de communication. Cette identification portera sur divers éléments tels que les composantes concernées (par ex. les types d'infrastructures protégées), les parties prenantes concernées (propriétaires ou opérateurs d'infrastructures, groupes publics ou privés d'intervention en cas d'urgence, etc.), les utilisateurs des infrastructures, les domaines critiques pour lesquels ces infrastructures sont employées (énergie, santé, etc.), les responsabilités en matière de gestion des risques de chaque partie prenante concernée, les activités de coordination nécessaires, les nécessaires schémas d'escalade au niveau national, etc. Il sera procédé à un premier classement de ces éléments en fonction de leur valeur, leur impact et leur profil de risque. Les documents produits alimenteront le lot de travaux 1.4 et faciliteront la définition des scénarios requis en vue des exercices paneuropéens de résilience. C'est pourquoi l'interface établie entre cette activité et	

les activités du PTPA 1 sera nécessaire, l'une et les autres concernant la coordination du groupe de travail mais aussi la planification et la structure des livrables du groupe de travail. En possession de ces informations, les parties prenantes intéressées seront en mesure de suivre les évolutions nationales dans ce domaine et de décider quelles activités seront nécessaires pour établir ou renforcer la préparation en matière de gestion nationale des risques. De plus, ces informations formeront la base des activités d'inventaire à mener dans différents États membres et de la détermination d'une feuille de route pour les actions futures dans ce domaine. Concernant l'exercice de résilience paneuropéen, la future liste des éléments liés à la PIIC, fondée sur les risques reconnus, constituera une contribution importante en vue de la définition des scénarios d'exercice.
RÉSULTATS ET CALENDRIER:
Documentation des éléments/domaines identifiés concernant la préparation en matière de gestion nationale des risques (d'ici au 4^{e} trimestre 2010)
PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:
Conseil d'administration, groupe permanent des parties prenantes, ALN, Commission européenne, États membres, experts (industrie, universités, recherche)
RESSOURCES POUR 2010 (personnes-mois et budget)
• 80 000 euros • 11 personnes-mois
LOT DE TRAVAUX PROPOSÉ PAR:
ENISA
BASE JURIDIQUE
Règlement ENISA, article 3, points a), c), d),e), f), g), i) et k)

2.4. AP 1: Identité, responsabilité et confiance dans l'internet du futur

NOM DU THÈME:
AP 1: Confiance et vie privée dans l'internet du futur
DESCRIPTION DU PROBLÈME À RÉSOUDRE:
Depuis l'avènement d'internet, toute personne a la possibilité de vivre deux vies en parallèle: l'une dans le monde réel et l'autre dans le monde virtuel. Ces dernières années, on a observé une tendance, apparue d'abord dans la communauté de la recherche mais maintenant également dans les offres commerciales, à augmenter les interactions entre ces deux mondes, ce qui se traduit notamment par la possibilité d'accéder à des informations du monde réel par le biais de services internet. Cette tendance nous amènera à une situation où des nœuds de capteurs et de déclencheurs constitueront la majorité des nœuds connectés de l'internet du futur, formant son aspect «monde réel» et, en même temps, augmentant la quantité d'informations accessibles par recherche sur internet. En plus de cet internet du monde réel, l'internet des objets (IdO) profile une autre ligne d'évolution parallèle de l'internet du futur. Évolution de l'actuelle technologie RFID, l'IdO consiste en réseaux de nœuds qui interagissent avec des objets munis d'étiquettes. *L'internet du futur (IF), bien que se présentant encore en couches, sera soumis à une série de dépendances transversales, ce qui entraînera une complexité accrue et une répartition des responsabilités. Il se caractérisera par une échelle bien plus vaste que l'internet actuel, surtout en raison de l'énorme extension de son champ d'application, elle-même le fruit de l'inclusion d'une multitude d'entités connectées de types divers. L'IF va probablement susciter l'apparition de comportements spontanés et émergents et d'utilisations non anticipées. L'apparition d'entités, services et scénarios commerciaux nouveaux sera la règle plutôt que l'exception. Il en résultera un environnement numérique omniprésent, composé d'une multiplicité d'infrastructures, de terminaux et de technologies hétérogènes connectés entre eux. Les utilisateurs interagiront par le biais de l'IF pendant toute leur vie, dans des rôles variés et dans des communautés et contextes socio-économiques différents. Chacune de ces situations imposera l'utilisation de différentes identités, des besoins de protection et des exigences de confiance.*[9] Sans aucun doute, la sécurité, la vie privée et la confiance sont cruciales pour tout service, application ou transaction passant par les réseaux publics de communication. Ces aspects devraient prendre encore davantage d'importance dans le cadre de grands systèmes distribués offrant des liens vers le monde réel, comme l'internet du futur va sans doute le faire. Dans ce contexte, les défis clés à relever consistent notamment à assurer l'intégrité de l'information, protéger les sources d'information et instaurer la confiance vis-à-vis des personnes mais aussi des objets, capteurs et déclencheurs.
DESCRIPTION DE L'APPROCHE RETENUE POUR RÉSOUDRE LE PROBLÈME:
L'objectif général de cette action préparatoire est de «veiller à ce que l'Europe maintienne un degré élevé de sécurité et de confiance parmi les utilisateurs et l'industrie concernant les infrastructures et les fournisseurs de services de TIC, tout en limitant les menaces susceptibles de peser sur les libertés civiles et la vie privée». L'ENISA compte atteindre cet objectif des façons suivantes: 1) Examiner et évaluer l'impact et les conséquences potentielles des menaces découlant de l'introduction des technologies émergentes, et déterminer le rôle de la confiance et de la responsabilité, notamment dans les infrastructures. L'ENISA étudiera des modèles de services électroniques liés à la sécurité et, à cet égard, prendra en considération les méthodes disponibles pour la gestion ou la suppression, avec consentement de l'utilisateur, des données à caractère personnel, la diffusion de méthodes de gestion – toujours avec consentement de l'utilisateur – dans des environnements multiples, et leur utilisation possible dans des scénarios de services de l'internet du futur.

[9] Document de position sur la confiance et l'identité dans l'internet du futur, Assemblée sur l'internet du futur, Madrid, 9 décembre 2008

2) Suivre le développement et le déploiement de technologies permettant un accès aux données respectueux de la vie privée, de mécanismes assurant une divulgation minimale, de systèmes d'identités perfectionnés, d'une offre de services d'identité respectueux de la vie privée, d'exigences politiques et leur application, et d'un contrôle de l'utilisation fondé sur une informatique de confiance et une sécurité de bout en bout. Réaliser un exercice d'inventaire en considérant les importantes tendances et/ou questions liées à la vie privée.
3) Développer des initiatives politiques et de bonnes pratiques orientées sur l'atteinte d'un équilibre entre transparence et responsabilité. Cette ambition englobe l'élaboration d'exigences relatives au rapprochement des modèles existants d'authentification électronique, de lignes directrices et de recommandations pour les réglementations nécessaires en matière de vie privée et de confiance, en fonction des besoins, ainsi que d'un modèle de gouvernance concernant la supervision et l'accréditation.
4) Coopérer étroitement avec la Commission (en particulier avec la DG INFSO.F5 et la DG INFSO.H2 afin d'assurer un échange régulier d'informations et l'exploitation des synergies qui seront identifiées au fur et à mesure de l'avancement de l'initiative.

L'ENISA réalisera le travail préparatoire en vue des prochaines années en examinant un certain nombre de technologies du domaine concerné, l'état d'avancement de leur déploiement et les initiatives politiques touchant à la confiance et à la vie privée. Étant donné la complexité de ce sujet, l'action préparatoire s'étalera sur deux années, 2010 et 2011.

IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.)

Objectif SMART: D'ici à 2012, la Commission et au moins 50 % des États membres ont fait usage des recommandations de l'ENISA dans leur processus d'élaboration de politiques.

ICP: Commission (oui/non), % d'États membres

OBJECTIFS SUPÉRIEURS APPUYÉS PAR LE PROGRAMME

Donner au secteur public et à l'industrie des TIC confiance dans l'internet du futur
Faciliter le marché intérieur des communications électroniques en aidant les institutions à choisir les meilleures réglementations et mesures à prendre
Renforcer le dialogue sur la vie privée et la confiance (y compris dans les infrastructures) entre les diverses parties prenantes dans l'UE
Intensifier la coopération entre les États membres en vue de réduire leurs différences en matière d'initiatives politiques

PARTIES PRENANTES + BÉNÉFICIAIRES

Autorités réglementaires nationales, gouvernements d'États membres ainsi que responsables et décideurs de l'UE, opérateurs de réseaux et fournisseurs de services, associations de fournisseurs et d'auditeurs, vendeurs d'équipement de réseau

POURQUOI L'ENISA?

L'ENISA est bien placée pour offrir au grand public et à l'industrie un degré élevé de sécurité et de confiance dans les infrastructures et les services de TIC.

De par sa nature, l'internet ne connaît pas les frontières nationales; les défis dans ce domaine ne peuvent donc être relevés «isolément» ni sans coordination entre les États membres de l'UE. Par sa désignation, l'ENISA est bien placée pour promouvoir et faciliter des politiques, activités et procédures conjointes dans ce domaine au niveau de l'Union européenne.

2.4.1 L.T. A.P. 1.1 – Inventaire des mécanismes d'authentification et de respect de la vie privée

Nom du PTPA:	
Confiance et vie privée dans l'internet du futur	
NOM DU LOT DE TRAVAUX:	
L.T. A.P. 1.1: Inventaire des mécanismes d'authentification et de respect de la vie privée	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: Plus de 5 références aux livrables > **Objectif SMART**: Plus de 20 États membres participent aux exercices d'inventaire	**ICP:** nombre de références faites **ICP:** nombre d'États membres
DESCRIPTION DU LOT DE TRAVAUX	
La notion d'identité dans les applications et services des TIC évolue rapidement, et de nombreux concepts qui y sont associés, comme la «confiance», pourraient avoir des effets profonds sur la manière dont les infrastructures et les services seront assurés à l'avenir. Le succès des sites de réseaux sociaux, entre autres, démontre l'existence de nombreuses possibilités d'abus par utilisation inappropriée des informations à caractère personnel. Si on néglige ces préoccupations, le public perdra sa confiance dans les services de TIC et l'innovation et la croissance seront entravées. Les travaux réalisés précédemment par l'ENISA dans ce domaine ont indiqué que l'un des plus gros obstacles à surmonter à moyen terme est la différence d'exigences de sécurité et de vie privée qu'il y a dans les États membres de l'UE concernant diverses applications. L'ENISA continuera à travailler sur ce thème en collaborant avec des initiatives européennes de premier plan, notamment l'IDABC, le consortium STORK et les groupes de travail du CEN. À cet égard, le but sera d'identifier les bases nécessaires pour établir des services sûrs dans toute l'Europe, ce qui débouchera sur l'établissement de bonnes pratiques et de recommandations pour les technologies liées à la sécurité des services ainsi qu'à l'authentification, l'autorisation et la responsabilité électroniques. Dans ce contexte, plusieurs méthodes d'authentification, notamment les cadres d'identification basés sur le web et les méthodes d'authentification à base de jetons informatiques, doivent être comparées en tenant compte des exigences des importants services électroniques en Europe. La gestion des identités multiples forme un autre domaine particulièrement intéressant. Ici, l'«identité» est considérée dans son sens large (identité électronique, identité fédérée, RFID, avatars, etc.). Les environnements applicatifs qui pourraient être étudiés sont les mondes virtuels en ligne, dans lesquels la notion d'anonymat mérite d'être explorée. Enfin, l'exigence européenne de notification des violations des données pour le secteur des communications électroniques qui a été introduite dans la révision de la directive «vie privée et communications électroniques» (2002/58/CE) revêt une grande importance. En effet, ce changement est susceptible d'accroître le degré de sécurité des données en Europe et de rassurer les citoyens sur le traitement et la protection de leurs données à caractère personnel par les opérateurs du secteur des communications. Dans ce contexte, l'ENISA entend passer en revue la situation actuelle et élaborer un ensemble cohérent de lignes directrices relatives aux mesures et procédures de mise en œuvre technique telles que décrites à l'article 4 de la version révisée de la directive 2002/58/CE.	
RÉSULTATS ET CALENDRIER:	
• Rapport identifiant les méthodes de gestion d'identités multiples (4e trimestre 2010) • Rapport présentant les derniers progrès dans le déploiement des identités électroniques dans les secteurs privé et public des États membres, et identifiant les tendances et les incitations possibles (4e trimestre 2010) • Inventaire des pratiques en matière de notification des violations de données dans divers secteurs (4e trimestre 2010) Les étapes suivantes liées aux activités citées ci-dessus, à réaliser en 2011 au cas où cette action préparatoire serait transformée en un programme thématique pluriannuel, sont notamment:	

• Bonnes pratiques et recommandations pour les technologies liées à la sécurité des services et à l'authentification • Lignes directrices relatives aux mesures et procédures de mise en œuvre technique telles que décrites à l'article 4 de la directive 2002/58/CE
PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:
Vendeurs d'équipement de mise en réseau, autorités réglementaires nationales (ARN), fournisseurs de services, institutions de R&D industrielles, universités et centres de recherche, plates-formes technologiques européennes.
RESSOURCES POUR 2010 (personnes-mois et budget)
• 9 personnes-mois[10]
LOT DE TRAVAUX PROPOSÉ PAR:
ENISA
BASE JURIDIQUE
Règlement ENISA, article 3, points a), b), c), f) et k)

[10] À la date de rédaction du présent document, l'Agence n'est pas en mesure d'engager des ressources financières dans cette action préparatoire. Néanmoins, les ressources requises (90 000 euros) pourraient être obtenues dans le courant de l'année.

2.4.2 L.T. A.P. 1.2 – Inventaire de modèles de services soutenant les services électroniques

Nom du PTPA:
Confiance et vie privée dans l'internet du futur
NOM DU LOT DE TRAVAUX:
L.T. A.P. 1.2: Inventaire de modèles de services soutenant les services électroniques
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):
Objectif SMART: Identification et évaluation de plus de 5 modèles de services — **ICP:** nombre de modèles de services évalués **Objectif SMART:** Plus de 5 références aux livrables — **ICP:** nombre de références faites
DESCRIPTION DU LOT DE TRAVAUX
L'objectif principal de cette activité est de mener un exercice d'inventaire sur les modèles existants de services électroniques et leurs caractéristiques de sécurité, en donnant une indication de l'équilibre entre leurs aspects relatifs à la vie privée, la responsabilité, le consentement et le suivi. Aujourd'hui, les environnements applicatifs en ligne se caractérisent par une pléthore de modèles de sécurité «personnalisés», taillés à la mesure des diverses catégories d'applications dans lesquelles ils opèrent. Il est nécessaire de déterminer comment les utilisateurs devraient employer les différents types de services électroniques. En 2010, l'ENISA étudiera des modèles de sécurité de services électroniques et leurs performances dans des environnements hautement distribués tels que l'internet d'aujourd'hui. De plus, l'ENISA explorera diverses façons d'assurer le respect de la vie privée et la responsabilité sur internet, passera en revue les principales méthodes employées, étudiera leur cartographie par rapport aux architectures sous-jacentes et estimera leur degré d'efficacité et de performance. L'ENISA travaillera également à l'élaboration de recommandations sur l'emploi de certains modèles de services dans des environnements et des architectures donnés. À cet effet, il s'agira aussi de rédiger des lignes directrices concernant les actions nécessaires dans le domaine de la vie privée et de la confiance.
RÉSULTATS ET CALENDRIER:
• Catalogue des modèles de services actuels et de leurs questions sécuritaires dans différentes architectures (4e trimestre 2010) • Évaluation des modèles de services identifiés et recommandations pour des architectures spécifiques (4e trimestre 2010)
PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:
Autorités réglementaires nationales (ARN), Commission européenne, fournisseurs de services, universités et centres de recherche, CEPD, plates-formes technologiques européennes.
RESSOURCES POUR 2010 (personnes-mois et budget)
• 9 personnes-mois[11]
LOT DE TRAVAUX PROPOSÉ PAR:
ENISA
BASE JURIDIQUE
Règlement ENISA, article 3, points a), b), c), f) et k)

[11] À la date de rédaction du présent document, l'Agence n'est pas en mesure d'engager des ressources financières dans cette action préparatoire. Néanmoins, les ressources requises (90 000 euros pour les ateliers, expertise-conseil, gestion des groupes d'experts, publications électroniques et imprimées) pourraient être obtenues dans le courant de l'année (grâce à la contribution des pays de l'EEE).

2.5. AP 2: Identification des moteurs et des cadres de la coopération sectorielle de l'UE en matière de SRI

NOM DU THÈME:
AP 2: Identification des moteurs et des cadres de la coopération sectorielle de l'UE en matière de SRI
DESCRIPTION DU PROBLÈME À RÉSOUDRE:
Un nombre croissant de menaces sur la sécurité des réseaux et de l'information (SRI) font intervenir des combinaisons sophistiquées de protocoles de réseaux et services. Les formes de protection traditionnelles simplement basées sur de puissants pare-feu disposés autour de réseaux d'entreprise individuels ne sont plus suffisantes pour empêcher les intrus de pénétrer les réseaux et d'y voler ou endommager les actifs électroniques clés des entreprises ou d'autres organisations. Cette situation constitue un défi fondamental pour les organisations exerçant des activités commerciales en ligne. En réponse à la demande du marché concernant des solutions à ce problème, on assiste à un accroissement de la coopération entre les fournisseurs de réseaux et de services concernant le développement et la fourniture de services de SRI. Les actifs incorporels revêtant de plus en plus d'importance pour la création de valeur, les entreprises de haute technologie, tant petites que grandes, ont également de bonnes raisons de s'occuper des défis en matière de SRI en coopération avec des agences publiques. Les entreprises individuelles sont évidemment soumises à certaines obligations légales de coopération avec les autorités publiques dans des domaines tels que la protection et la conservation des données. Toutefois, en raison de la nature complexe et parfois juridiquement ambiguë des atteintes à la SRI (du moins au début), il pourrait s'avérer nécessaire d'intensifier les formes de coopération plus volontaires, globales et proactives entre les secteurs des chaînes d'approvisionnement, cela si l'on tient à éviter que l'exploitation des failles de sécurité de cette chaîne ne cause des perturbations économiques potentiellement étendues. Toutefois, pour être efficaces, les formes de coopération de ce type doivent se baser sur une estimation réaliste de la capacité de chaque partie à relever les défis de SRI par rapport avec leurs responsabilités et capacités commerciales ou réglementaires légitimes. Faute de quoi, les solutions risquent d'être fragmentées, inadéquates, disproportionnées ou irréalistes au regard des besoins des parties concernées ou de ce qu'elles peuvent offrir. Pourtant, pour une grande diversité d'importantes questions de politique publique, les problèmes pourraient provenir de la seule coopération du côté offre si les moteurs du côté demande ne sont pas nettement définis ou les défaillances du marché clairement identifiées. Néanmoins, on sait très peu de choses sur les conditions opérationnelles, commerciales et/ou réglementaires qui ont pour effet de décourager, faciliter ou encourager la coopération en matière de SRI entre les divers secteurs. Or, la coopération avec les autorités publiques concernant l'élaboration d'outils de services, de services ou de cadres coopératifs peut s'avérer mutuellement utile ou souhaitable du point de vue du commerce ou de la politique publique. Si les organisations concernées sont appelées à assumer des exigences réglementaires cohérentes, directes et efficaces ainsi qu'une coordination entre le public et le privé, il importe d'intégrer des approches nationales, communautaires et internationales optimisées. À cause de la complexité croissante des menaces sur la sécurité, il est rarement possible pour toute entité à tout niveau d'y répondre de façon isolée. Les actions des intervenants dans divers domaines de responsabilité à tout niveau peuvent influencer la capacité d'action des autres, ce qui peut se traduire par une diminution de l'efficacité globale. Les tentatives de coopération au niveau paneuropéen ou international peuvent en outre être en contradiction avec les exigences réglementaires nationales, à moins que les partenariats ne reçoivent des sanctions ou soutiens juridiques explicites des agences sectorielles publiques au niveau communautaire et international. Alors que les incitations générales à la coopération au sein du secteur privé et entre les secteurs public et privé sont parfois très étendues, les obstacles à leur mise en œuvre peuvent également s'avérer coriaces. L'analyse de ces obstacles peut aider à déterminer comment les cadres paneuropéens pourraient créer

des incitations commerciales, économiques et réglementaires afin que divers acteurs de la chaîne d'approvisionnement (opérateurs de réseaux, fournisseurs de logiciels et de services, associations d'utilisateurs et agences publiques) coopèrent entre eux de façon à faciliter les moteurs du marché là où il y en a et en pleine conformité avec toute la gamme d'exigences de la politique publique en cas de défaillance du marché. L'AP proposée ici vise donc à déterminer avec clarté quelle est la *meilleure façon* d'obtenir des acteurs pertinents l'engagement d'entreprendre une action collective pour relever les défis de SRI au niveau paneuropéen.

DESCRIPTION DE L'APPROCHE RETENUE POUR RÉSOUDRE LE PROBLÈME:

L'AP déterminera, dans le cadre du développement d'une série de services de la chaîne d'approvisionnement de la SRI, où les obstacles commerciaux, économiques et/ou réglementaires à la coopération sectorielle et les moteurs de cette coopération, ainsi que les incitations aux partenariats des secteurs public et privé, sont plus forts ou plus faibles. Comme décrit dans le LT AP 2.1, les travaux commenceront par la détermination des exigences de services de SRI des acteurs du secteur privé dans deux ou trois secteurs. Ces exigences seront considérées par rapport aux travaux de l'ENISA sur la résilience des IIC, et l'orientation commerciale et économique de l'AP *complétera* l'orientation plus opérationnelle et technologique des tâches du PTPA 1 du programme de travail 2010 en se centrant sur les exigences du côté demande concernant la coopération des entreprises en tant qu'intermédiaires ou utilisatrices finales des services de SRI de bout en bout dans la chaîne d'approvisionnement. La relation entre les questions générales et sectorielles sera développée selon les étapes suivantes:

1. Identification de la menace générale, du modèle commercial et des conditions de marché qui peuvent amener les acteurs du côté demande de divers secteurs (les utilisateurs de services de réseaux de grandes entreprises et de PME) à exiger une coopération intersectorielle accrue sur les questions de SRI essentielles.
2. Identification des manières et de l'étendue avec lesquelles ces exigences peuvent susciter un besoin de responsabilités, engagements et récompenses spécifiques pour les fournisseurs d'infrastructures, de logiciels et de services de sécurité.
3. Identification des outils, services ou cadres coopératifs qui constituent des pratiques particulièrement bonnes et peuvent être développés entre les secteurs public et privé au niveau paneuropéen afin de répondre à ces exigences.

Ces étapes seront exécutées en rapport avec, entre autres initiatives, l'engagement de l'ENISA concernant une communauté d'échange d'information et d'alerte en matière financière (FI-ISAC) ainsi que l'élaboration d'un outil en ligne pour les micro-entreprises et du projet suédois et néerlandais *Multipurpose Information Managements and Exchange for Robustness* (projet polyvalent de gestion et d'échange d'informations - MIMER). L'exécution de ces étapes sera facilitée par la participation des membres du groupe permanent des parties prenantes de l'ENISA – à la fois les membres individuels mais aussi ceux des entités qu'ils représentent – ainsi que par celle de la section Relations avec les parties prenantes de l'ENISA et de réseaux d'autres secteurs et d'associations sectorielles nationales.

La majeure partie des travaux de cette AP s'effectuera comme annoncé dans le LT AP 2.1. De plus, pendant les 1er et 2e trimestre 2010, l'Agence réalisera une analyse des questions clés relatives aux structures de coopération nationales, communautaires et internationales en matière de SRI pour les acteurs des secteurs public et privé. Cette analyse se fera en coordination étroite avec les travaux et l'analyse du PTPA 1 concernant la résilience des réseaux mais aussi avec un rapport indépendant basé sur des interviews approfondies, par un consultant, de représentants clés des États membres et du secteur privé participant à des projets coopératifs ainsi qu'avec les rapports pays et le répertoire Who-is-Who du LT 2.3. L'objectif de cet exercice sera de déterminer avec précision à quel niveau l'engagement de l'ENISA pourrait le mieux soutenir les objectifs politiques de la Commission et des États membres.

Le rapport et l'évaluation (y compris du LT AP 2.1) seront élaborés et testés pendant trois ateliers auxquels participeront des participants de la chaîne d'approvisionnement des deux ou trois secteurs concernés. Ces ateliers auront lieu dans les États membres ou les installations de l'ENISA durant les 2e et 3e trimestres 2010. Enfin, pendant le 4e trimestre 2010, l'ENISA réunira les parties prenantes concernées à l'occasion d'un atelier final dont l'objectif sera d'examiner les conclusions générales des travaux et de suggérer les lignes d'actions possibles pour après 2010.

IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.)	
Objectif SMART: Détermination, dans le cadre du développement d'une série de services de la chaîne d'approvisionnement de la SRI, des points où les obstacles commerciaux, économiques et/ou réglementaires à la coopération sectorielle et les moteurs de cette coopération, ainsi que les incitations aux partenariats des secteurs public et privé, sont plus forts ou plus faibles.	**ICP:** Participation à l'élaboration d'initiatives coopératives intersectorielles dans au moins 3 chaînes d'approvisionnement dans au moins 2 États membres de l'UE. **ICP:** Identification des exigences pour la participation du secteur public à l'élaboration des outils, services ou cadres coopératifs constituant de bonnes pratiques par les acteurs du côté demande dans au moins 2 chaînes d'approvisionnement.
Objectif SMART: Détermination de la manière dont des initiatives coopératives pourraient être développées dans au moins 2 domaines de travail de l'ENISA après 2010.	**ICP:** nombres d'outils, services ou cadres coopératifs constituant de bonnes pratiques identifiés pour un suivi dans le cadre des travaux de l'ENISA après 2010.

OBJECTIFS SUPÉRIEURS APPUYÉS PAR LE PROGRAMME:

- Faciliter le marché intérieur des communications électroniques en aidant les institutions à choisir les meilleures réglementations et mesures à prendre
- Renforcer le dialogue entre les diverses parties prenantes dans l'UE sur la résilience des réseaux, la sécurité des services et logiciels, la vie privée et la confiance.
- Intensifier la coopération entre les États membres en vue de réduire leurs différences en matière d'initiatives politiques.
- Donner aux secteurs public et privé européens confiance dans l'internet du futur

PARTIES PRENANTES + BÉNÉFICIAIRES

États membres, responsabilités politiques et décideurs de l'UE, autorités réglementaires nationales, groupe permanent des parties prenantes, entreprises des chaînes d'approvisionnement paneuropéennes, diverses «communautés du secteur privé» dans l'industrie, utilisateurs/consommateurs et associations professionnelles.

POURQUOI L'ENISA?

L'ENISA est bien placée pour donner aux acteurs des secteurs public et privé une grande confiance concernant l'élaboration d'une approche intersectorielle du développement d'un cadre applicable à la coopération paneuropéenne en matière de SRI. Elle peut en effet compter sur une représentation multipartite dans son groupe permanent des parties prenantes, sur des réseaux de groupements d'entreprises et professionnels (à l'échelle de l'UE et des États membres), et réalisent déjà des travaux dans le domaine de la sécurité des infrastructures et des services de TIC. L'ENISA est la seule agence officielle capable de s'atteler aux problèmes relatifs aux chaînes d'approvisionnement paneuropéennes et aux lacunes des modèles de coopération pouvant exister à ce niveau. Elle travaille déjà avec des organisations internationales – ou en leur sein – qui s'occupent de ces problèmes (OCDE, ICANN, UIT et pays tiers).

RESSOURCES POUR 2010 (personnes-mois et budget)

- 105 000 euros
- 10 personnes-mois

2.5.1 L.T. A.P. 2.1 – Incitations et exigences de responsabilité pour les cadres de gouvernance multipartite en matière de SRI dans les communautés de fournisseurs et d'utilisateurs de TIC

Nom du PTPA	
Moteurs et cadres de la coopération sectorielle de l'UE en matière de SRI	
NOM DU LOT DE TRAVAUX:	
L.T. A.P. 2.1: Incitations et exigences de responsabilité pour la coopération multipartite en matière de SRI dans les communautés de fournisseurs et d'utilisateurs de TIC	
IMPACT SOUHAITÉ (ICP liés aux objectifs S.M.A.R.T.):	
Objectif SMART: Identification des conditions des menaces qui incitent les acteurs privés à établir des cadres coopératifs de responsabilités partagées en matière de SRI avec les acteurs du secteur public au niveau paneuropéen.	**ICP:** Participation à l'établissement par des acteurs privés d'un cadre paneuropéen avec le secteur public dans au moins 2 secteurs d'au moins 2 États membres de l'UE.
Objectif SMART: Identification des conditions commerciales et du marché qui, pour les entreprises du côté demande (grandes entreprises et PME), peuvent entraîner le besoin d'un cadre public-privé de coopération intersectorielle en matière de SRI.	**ICP:** Défaillance du marché pour ce qui est de l'offre intersectorielle de services de SRI pour au moins 2 secteurs du côté demande, sur les marchés des grandes entreprises et/ou PME, dans au moins 2 États membres de l'UE.
Objectif SMART: Identification des outils ou services constituant de bonnes pratiques à développer pour soutenir le fonctionnement de tels cadres coopératifs.	**ICP:** Numéro d'outils et/ou services constituant de bonnes pratiques identifiés pour soutenir les cadres coopératifs applicables aux grandes ou petites entreprises dans au moins 2 secteurs.
DESCRIPTION DES TÂCHES:	
Une des premières tâches de cette AP consiste à déterminer où les obstacles et les incitations à la coopération intersectorielle sont plus forts ou moins forts, quelles sont les possibilités de réussite à court terme ou à moyen terme et si, en conséquence, les partenariats public-privé sont plus ou moins nécessaires. Ce lot de travaux explorera donc les exigences de SRI de différents groupes d'acteurs du secteur privé, ainsi que les incitations concernant leur engagement dans des cadres multipartites. En particulier, il analysera dans quelle mesure les exigences de SRI des utilisateurs commerciaux de services de réseau peuvent ou non affecter la coopération entre les fournisseurs de logiciels et de services et les opérateurs de réseaux quant au développement et à la fourniture de service de SRI. Dans au moins une chaîne d'approvisionnement, le lot de travaux visera à faire la distinction entre la réussite d'une fourniture de services et la coopération du côté demande pour les grands utilisateurs commerciaux par rapport aux PME. Concernant ces dernières, on tâchera également de voir si la participation d'organisations de multiplicateurs à la définition des exigences des PME (au lieu d'un simple engagement individuel vis-à-vis de fournisseurs de services de SRI) peut augmenter la capacité de susciter un changement. Enfin, il déterminera si, dans les cas où les exigences des utilisateurs ne sont pas satisfaites, la participation d'acteurs du secteur public au développement d'outils ou de services constituant de bonnes pratiques peut faciliter la coopération intersectorielle demandée par les utilisateurs. Pendant les 1er et 2e trimestres 2010, l'Agence réalisera deux études des exigences de SRI parmi les utilisateurs commerciaux, notamment les PME de haute technologie à traiter dans au moins une des deux études. Ces deux études auront trait à ces secteurs dans au moins deux États membres. Les projets d'études, y compris les observations préliminaires, seront présentés lors des deux ateliers organisés dans le cadre de la rubrique générale AP 2, qui auront lieu dans les États membres ou les installations de l'ENISA durant les 2e et 3e trimestres 2010. Pendant le 4e trimestre 2010, l'ENISA réunira les parties prenantes concernées à l'occasion d'un atelier final dont l'objectif sera d'examiner les conclusions générales des travaux et de suggérer les lignes d'actions possibles pour après 2010.	

RÉSULTATS ET CALENDRIER
• Études sectorielles du côté demande: 1er et 2e trimestres • Rapport des consultants: 4e trimestre • Ateliers: 2e, 3e et 4e trimestres
PARTIES PRENANTES NÉCESSAIRES POUR SOUTENIR ACTIVEMENT CE LOT DE TRAVAUX:
États membres: conseil d'administration, agents de liaison nationaux; groupe permanent des parties prenantes; réseaux de diverses «communautés thématiques» (secteur privé: industrie, utilisateurs/consommateurs, universités, etc.), entreprises individuelles.
RESSOURCES POUR 2010 (personnes-mois et budget)
• 105 000 euros • 10 personnes-mois
LOT DE TRAVAUX PROPOSÉ PAR:
ENISA
BASE JURIDIQUE
Règlement ENISA, article 3, points c) et d)

Résumé des programmes thématiques pluriannuels et des lots de travaux

PTPA 1	**Améliorer la résilience des réseaux de communication électroniques européens**	**Ligne budgétaire**	**Budget**	**Personnes-mois**	**Nouvelle activité**
LT 1.1	Aider les parties prenantes à déployer les guides ENISA de bonnes pratiques en matière de partage des informations et de signalement des incidents.	3510	100 000	11,5	Révisée
LT 1.2	Aider les fournisseurs à améliorer la résilience de leurs réseaux.	3510	150 000	13,5	Révisée
LT 1.3	Examen d'actions innovantes	3520	195 000	17,5	NON
LT 1.4	Responsabiliser les parties prenantes en vue du premier exercice paneuropéen	3520	100 000	13,5	Révisée
	TOTAL		**545 000**	**56**	
PTPA 2	**Développer et entretenir des modèles de coopération**	**Ligne budgétaire**	**Budget**	**Personnes-mois**	**Nouvelle activité**
LT 2.1	Plate-forme de coopération pour la communauté de sensibilisation	3310	60 000	24	NON
LT 2.2	Cercle de compétence en matière de sécurité et partage de bonnes pratiques pour les communautés CERT	3300	135 000	24	NON
LT 2.3	Facilitation de l'échange de bonnes pratiques de SRI au niveau européen	3320	120 000	7	NON
	TOTAL		**315 000**	**55**	
PTPA 3	**Identifier les risques émergents pour renforcer la confiance**	**Ligne budgétaire**	**Budget**	**Personnes-mois**	**Nouvelle activité**
LT 3.1	Cadre pour l'évaluation et la discussion des risques émergents – Analyse de scénarios spécifiques	3500	120 000	16	NON
LT 3.2	Maintenance du cadre des risques émergents et futurs	3500	35 000	3	NON
LT 3.3	Renforcement de la préparation en matière de gestion nationale des risques	3500	80 000	11	OUI
	TOTAL		**235 000**	**30**	
AP 1	**Identité, responsabilité et confiance dans l'internet du futur**	**Ligne budgétaire**	**Budget**	**Personnes-mois**	**Nouvelle activité**
LT AP 1.1	Suivi et évaluation des risques et menaces pour la résilience, la vie privée et la confiance découlant de l'introduction des technologies émergentes	3520	0	9	OUI
LT AP 1.2	Développement d'initiatives politiques orientées sur l'atteinte d'un équilibre entre vie privée, responsabilité, consentement et suivi	3520	0	9	OUI
	TOTAL		**0**	**18**	
AP 2	**Identification des moteurs et des cadres de la coopération sectorielle de l'UE en matière de SRI**	**Ligne budgétaire**	**Budget**	**Personnes-mois**	**Nouvelle activité**
LT AP 2.1	Incitations et exigences de responsabilité pour les cadres de gouvernance multipartite en matière de SRI dans les communautés de fournisseurs et d'utilisateurs de TIC	3520	105 000	10	OUI
	TOTAL		**105 000**	**10**	

	TOTAL (tous les PTPA)		**1 200 000**	**169**	

3 ACTIVITÉS HORIZONTALES

L'Agence accomplira un certain nombre d'activités nécessaires à son fonctionnement en plus des programmes thématiques pluriannuels. Celles-ci comprennent des activités de gestion de la stratégie et des affaires publiques de l'ENISA, de gestion des organes et groupes de l'ENISA, de gestion des relations avec les parties prenantes externes, de mesure de l'adoption des produits livrables de l'ENISA, de gestion des capacités internes de l'Agence, de développement des communications internes et d'élaboration du programme de travail.

3.1. Activités de développement de la gestion de la stratégie et des affaires publiques de l'ENISA

L'Agence élaborera une stratégie couvrant la période allant jusqu'à 2012 et au-delà. Les exigences stratégiques relatives à l'élaboration des programmes de travail annuels seront établies en parallèle avec le processus d'élaboration des programmes de travail.

L'Agence mènera des activités de communication et de contact afin d'accroître l'impact de son travail. En 2010, elle utilisera ses canaux de communication institutionnelle pour établir le contact avec des experts en SRI. Les activités de communication institutionnelle ont été restructurées selon les lignes budgétaires suivantes: activités de communication (44 000 euros), site web officiel de l'ENISA (20 000 euros), Rapport général d'activité et autres publications de l'ENISA (40 000 euros). Le contact avec les experts en SRI se fera au moyen de la Lettre trimestrielle de l'ENISA (40 000 euros), d'événements co-organisés (30 000 euros) et d'interventions d'experts de l'ENISA à des conférences et manifestations (ce qui ne nécessite pas de budget supplémentaire).

Base juridique: règlement ENISA, article 2, paragraphe 3, et article 3, points a), e), f) et k) et article 7, paragraphe 5, point a)

3.2. Gestion des organes et groupes de l'ENISA

L'Agence organisera des réunions du conseil d'administration (110 000 euros) et du groupe permanent des parties prenantes (100 000 euros, y compris les réunions informelles CA/GPP). Les activités à mener dans le cadre du PTPA couvriront également les activités des groupes de travail et la gestion du réseau des agents de liaison nationaux.

Base juridique: règlement ENISA, articles 5 et 6, article 7, paragraphe 4, points g), h) et i), et article 7, paragraphe 8

3.3. Gestion des relations avec les parties prenantes externes

L'Agence, en coopération étroite avec les services de la Commission, entretiendra et développera les relations avec les organes de l'UE, avec les représentants de l'industrie, des universités et des consommateurs, avec des pays tiers et des institutions internationales (par ex. UIT, IETF, et OCDE); elle étudiera la possibilité de soutenir des partenariats public-privé (PPP) qui réunissent

ces divers acteurs. En outre, l'ENISA identifiera des domaines d'intérêt communs et évaluera dans quelle mesure une collaboration avec ces acteurs est faisable pour certaines activités spécifiques de l'Agence (par ex. faciliter le dialogue sur le développement de logiciels sécurisés entre l'industrie et la Commission en tant que législateur). Ces activités nécessitent 410 000 euros pour les missions du personnel, 5 000 euros pour les frais de représentation, 3 000 euros pour les réunions du directeur exécutif et 10 000 euros pour d'autres réunions.

Base juridique: règlement ENISA, article 3, points c) et j) et article 7, paragraphe 4, points g) et h)

3.4. Gestion des capacités internes

«L'Agence continuera à entretenir et à enrichir la base de données Who-is-Who en concertation avec les secteurs public et privé (0 euro). L'Agence poursuivra ses activités sur la gestion interne des risques et la sécurité de l'information en développant sa capacité d'audit interne (25 000 euros). En outre, l'Agence maintiendra sa capacité de traduction (20 000 euros) de ses documents financiers officiels.»

Base juridique: règlement ENISA, article 7, paragraphe 4, point d)

3.5. Gestion de la communication interne à l'ENISA

L'Agence attache une grande importance au partage d'informations et à la coopération entre son personnel et sa direction et, d'une façon générale, entre tous les membres du personnel. Pour cela, l'Agence a établi différents canaux de communication interne et distribuera fréquemment sa lettre d'information interne, organisera des réunions hebdomadaires internes avec le personnel et assurera le partage d'informations via l'intranet.

Base juridique: règlement ENISA, article 7, paragraphe 4, points d) et f)

3.6. Élaboration du programme de travail

Chaque année, l'Agence établit son programme de travail annuel. Ce programme fait l'objet de consultations avec le groupe permanent des parties prenantes et est soumis à la décision du conseil d'administration. En principe, cette activité ne nécessite pas de budget spécifique.

Base juridique: règlement ENISA, article 7, paragraphe 5, point b), article 7, paragraphe 6, et article 9

Résumé des activités horizontales

AH 1	**Fourniture de conseil et d'assistance**	**Ligne budgétaire**	**Budget**	**Personnes -mois**	**Nouvelle activité**
AH 1.1	Coordination du traitement des demandes	3320	0	0,5	NON
AH 1.2	Réponse aux demandes	3320	0	0,5	NON
	TOTAL		**0**	**1,0**	
AH 2	**Activité de communication et de contact avec les parties prenantes de la SRI**	**Ligne budgétaire**	**Budget**	**Personnes -mois**	**Nouvelle activité**
AH 2.1	Élaboration de la stratégie	p.m.	0	2,0	Révisée
AH 2.2	Gestion des affaires publiques	p.m.	0	10,5	Révisée
AH 2.3	Activités de communication	3210	44 000	5.5	Révisée
AH 2.4	Site web officiel de l'ENISA	3220	20 000	21	NON
AH 2.5	Rapport général d'activités et publications de l'ENISA	3210	40 000	6	NON
AH 2.6	Lettre trimestrielle de l'ENISA	3240	40 000	4	NON
AH 2.7	Événements co-organisés	3200	30 000	4	NON
AH 2.8	Interventions d'orateurs	n.a.	0	11	NON
	TOTAL		**174 000**	**64**	
AH 3	**Gestion des organes et groupes de l'ENISA**	**Ligne budgétaire**	**Budget**	**Personnes -mois**	**Nouvelle activité**
AH 3.1	Conseil d'administration	3003	110 000	4	NON
AH 3.2	Groupe permanent des parties prenantes	3000	100 000	4	NON
AH 3.3	Coordination des groupes de travail	N/A	0	2	NON
AH 3.4	Réseau des agents de liaison nationaux	N/A	0	2	NON
	TOTAL		**210 000**	**12**	

AH 4	Gestion des relations avec les parties prenantes externes	Ligne budgétaire	Budget	Personnes-mois	Nouvelle activité
AH 4.1	Développement des relations avec les représentants de l'industrie, des universités et des consommateurs, avec des institutions internationales et des pays tiers	3330	0	4,5	NON
AH 4.2	Gestion des relations avec les organes de l'UE	3320	0	3,5	NON
AH 4.3	Missions du directeur exécutif	3015	35 000	0	NON
AH 4.5	Missions des départements opérationnels	3013	345 000	0	NON
AH 4.6	Missions du département administratif	3014	30 000	0	NON
AH 4.7	Coûts de représentation	3011	5 000	0	NON
AH 4.8	Réunions du directeur exécutif	3005	3 000	0	NON
AH 4.9	Autres réunions	3021	10 000	0	NON
	TOTAL		**428 000**	**8**	
AH 5	Gestion des capacités internes de l'ENISA	Ligne budgétaire	Budget	Personnes-mois	Nouvelle activité
AH 5.1	Base de données Who-is-Who	3320	0	0	NON
AH 5.2	Capacité d'audit interne de l'ENISA	3400	25 000	1	NON
AH 5.3	Traductions	3230	20 000	0	NON
	TOTAL		**45 000**	**1**	
AH 6	Gestion de la communication interne à l'ENISA	Ligne budgétaire	Budget	Personnes-mois	Nouvelle activité
AH 6.1	Lettre d'information interne de l'ENISA, réunions du personnel et partage d'informations via l'intranet	N/A	0	4	NON
	TOTAL		**0**	**4**	
AH 7	Élaboration du programme de travail	Ligne budgétaire	Budget	Personnes-mois	Nouvelle activité
AH 7.1	Élaboration du programme de travail 2011	n.a.	0	10	NON
	TOTAL		**0**	**10**	
	TOTAL (activités horizontales)		**857 000**	**100**	

4 FOURNITURE DE CONSEIL ET D'ASSISTANCE

Depuis 2006, l'Agence reçoit des demandes en provenance des États membres (8), de la Commission européenne (6) et d'autres organes européens (2) (voir tableau ci-après). L'Agence s'attend à recevoir de telles demandes en 2010 également. Cela confirme le rôle prévu pour l'ENISA aux articles 2, 3 et 10 du règlement.

L'article 6 des règles de fonctionnement interne concernant le traitement des demandes spécifie la procédure à appliquer aux demandes reçues. Pour les demandes éligibles, l'Agence définira des priorités sur la base de critères tels que la disponibilité de ressources, la continuité des actions à long terme, les engagements existants ainsi que la valeur ajoutée et l'impact attendus au niveau européen de la réponse à la demande.

En principe, les demandes reçues seront traitées selon le système «premier arrivé, premier servi». En cas de besoin, le directeur exécutif consultera sans délai le conseil de direction avant de prendre une décision sur les priorités.

Tableau: Demandes traitées entre décembre 2005 et juin 2009

Demandeur	Sujet	Budget (euro)	Personnel de l'ENISA [Personnes-mois]
1)CEPD	Facilitation de l'audit du système EURODAC	3 400	1,6
2)Commission	Évaluation des mesures de sécurité prises par les fournisseurs de communications électroniques	0	2,2
3)ARN Lituanie	Assistance à la création de CERT par l'organisation d'une formation pour CERT en Lituanie	6 745	0,8
4)Commission	Information en retour sur l'évaluation de l'impact sur la communication prévue	0	1,3
5)Commission	Conseil sur l'examen à mi-parcours de la directive sur les signatures électroniques	850	0,5
6)Commission	Conseil sur la gestion des CIE dans les services de la Commission	850	1,1
7) République tchèque	Évaluation des besoins de sécurité des systèmes d'information des administrations publiques	0	0,6
8a) Commission	Étude de la faisabilité d'un cadre pour la collecte de données	50 000	6,0
8b) Commission	Étude de la faisabilité d'un système d'échange d'informations et d'alerte à l'échelle européenne	25 000	4,0
9) Grèce	Conseil sur le cryptage et la téléphonie	0	0,1
10) Autriche	Coopération SBA-ENISA	0	0,1
11) Autriche	Gestion des risques et questionnaire d'analyse	0	1,0
12) Bulgarie	Facilitation de la coopération Hongrie-Bulgarie pour la création d'un CERT gouvernemental bulgare	0	1,0
13) Grèce	Création d'un CSIRT à FORTH-ICS	0	0,1
14) Autriche	Assistance pour la création d'un CERT par l'organisation d'une formation aux CERT	6 745	0,8
15) Parlement eur.	Conseil sur des questions de sécurité relatives à internet	0	0,5
16) Chypre	Assistance pour la création d'un CERT gouvernemental	0	0,5

5 ACTIVITÉS ADMINISTRATIVES

Le département administratif de l'ENISA s'efforce d'assurer la conformité des procédures administratives de l'Agence et de continuer à améliorer leurs fonctionnalités afin de fournir des services fiables. En 2010, ce département s'est fixé comme objectif d'augmenter la diversité et la qualité des services accessibles en ligne, en conformité avec les objectifs de conformité qui ont été concrétisés dans les normes de contrôle interne et les résultats des audits. À cet égard, la gestion électronique des tâches sera rendue possible dans de nouveaux domaines d'activité; une plus grande atténuation des risques sera appliquée afin d'assurer la continuité des activités. En 2010, le département administratif s'efforcera de:

- Augmenter la diversité et la qualité des services accessibles
- Atténuer les risques de mise en conformité
- Assurer la continuité des activités

En 2010, le département administratif s'efforcera de continuer à améliorer ses interactions avec les sections et fonctions de l'Agence qui ont une orientation de service horizontale comme la comptabilité et le contrôle interne. Le programme de travail 2010 continue à se référer aux activités de ces deux fonctions à côté de la planification des activités du département administratif.

5.1. Administration générale

Les tâches administratives générales contribuent à assurer la gestion et la mesure de l'efficacité du département administratif. Les tâches principales comprennent la planification, le conseil, la représentation, la communication d'informations et le contrôle des activités des différentes sections et du département tout entier. En 2010, les priorités de l'administration générale englobent:

- La planification pluriannuelle des activités
- Le contrôle de l'exécution du budget annuel
- La planification de la gestion électronique des tâches
- L'atténuation des risques de conformité
- La continuité des activités

Les principales activités prévues pour 2010 sont les suivantes:

Réf.	Détails	Livrables	Indicateurs de performance	Calendrier	Budget
1.1	Planification des activités administratives Représentation du DA	Planification des activités, orientation et gestion Définition des objectifs et des priorités Coordination avec les départements et sections de l'Agence Collaboration avec le personnel clé à la réalisation des objectifs de service Gestion des ressources humaines	Planification d'activités par section Orientation en vue d'atteindre des objectifs Plan de travail annuel Coordination des objectifs du personnel du DA Communication	En continu	0
1.2	Conseil et assistance au DE et aux chefs des départements TC, en fonction des besoins, sur toutes les questions administratives, y compris gouvernance, bonne gestion financière, gestion par activités, plans d'urgence,	Rapports au DE et collaboration avec les chefs de département et le personnel clé en fonction des besoins	Assistance continuelle au DE et aux chefs des départements TC Réponse en temps opportun aux demandes d'assistance Soutien à la mise en œuvre de contrôles internes et de systèmes de contrôle des actifs	Toutes les semaines	0

	continuité des activités, services juridiques et protection des actifs				
1.3	Assurer que des niveaux d'information appropriés sur l'utilisation des ressources de l'Agence soient	En fonction des besoins	Évaluation périodique des besoins d'information internes et externes du département	Tous les trois mois	0
	disponibles à tout moment Exploitation des données financières et des lignes de rapport au DA		Présentation de rapports et suivi		
1.4	Suivi des résultats d'audit concernant les pratiques et procédures administratives appliquées conformément au règlement financier, aux modalités d'exécution et au statut du personnel Collaboration avec la coordination des contrôles internes et la comptabilité Planification de la continuité des affaires Remboursements TVA	Mise à jour de documents et présentation de rapports d'activités Coordination avec des acteurs internes (Coordination des contrôles internes, comptabilité, section de gestion des risques) et externes (Cour des comptes, IAS etc.)	Mise en œuvre des recommandations des audits Amélioration constante des performances Gestion des risques	Tous les trois mois	0
1.5	Tâches organisationnelles générales	Classement, communication, appui aux sections au DA ou selon les besoins, mise en route d'activités financières selon les besoins	Volume d'activités Exécution en temps utile	En continu	0
1.6	Services de bureau	Administration de tâches horizontales spécifiques, comme traductions, gestion du matériel de bureau, logistique, gestion de bureau, sûreté et sécurité, courrier, véhicules	Volume d'activités Exécution en temps utile	En continu	384 000
1.7	Relations avec les autorités grecques	Contacts réguliers et conseil au DE sur les relations avec les États membres hôtes	Nombre de cas traités Réponses en temps utile	En continu	0
1.8	Traitement des demandes du personnel concernant la mise en œuvre de l'accord de siège (cartes ID spéciales, immatriculations de voitures, exonération de TVA, etc.).[12]	Traitement régulier des demandes d'exonération de TVA pour le personnel de l'Agence	Nombre de cas traités Réponses en temps utile	En continu	0

5.2. Finances

La section Finances est chargée de la planification du budget, de son exécution et du contrôle financier ainsi que de certaines parties de l'administration salariale, de la supervision et du soutien des missions. L'objectif de la section Finances est d'assurer la crédibilité des circuits financiers et de la planification du budget. Le contrôle étroit de la planification et de l'exécution du budget permet à l'Agence d'augmenter son taux d'utilisation du budget, au bénéfice de ses activités, et de compenser les contraintes budgétaires. En 2010, les priorités de la section Finances sont les suivantes:

- Planification du budget, notamment budgétisation basée sur des activités.
- Suivi de l'exécution et de la planification du budget.
- Soutien fonctionnel concernant la gestion électronique des tâches (ABAC, gestion des missions).

[12] Voir les activités de la direction concernant les relations avec les autorités de la République hellénique.

Les principales activités prévues pour 2010 sont les suivantes:

Réf.	Détails	Livrables	Indicateurs de performance	Calendrier	Budget
2.1	Ouverture et clôture du budget annuel et préparation des états budgétaires	L'arborescence budgétaire approuvée est ouverte, les crédits sont correctement affectés	Lignes budgétaires annuelles ouvertes et en exécution depuis la fin de la troisième semaine de l'exercice fiscal, gestion du compte de production et opérations de soutien effectuées à temps	Fin janvier et fin de la troisième semaine de décembre. Préparation jusqu'au 10 décembre	0
2 2	Exécution et consolidation des procédures internes et contrôles internes pour tous les circuits financiers, y compris les missions	Examen annuel des procédures internes et des contrôles internes. Contrôles réguliers de toutes les transactions financières	Lignes directrices et listes de contrôle révisées. Évaluation annuelle des risques effectuée. Contrôles mis à jour en conséquence. Sessions de formation visant à familiariser le personnel avec les procédures et les contrôles. Exécution des contrôles	Tous les trois mois	0
2.3	Rapports sur le budget annuel	Rapports mensuels	Rapport sur la situation budgétaire pour tous les domaines, titres et départements, selon les nécessités, y compris analyse des principaux aspects pertinents	Tous les mois (pour le mois précédent)	0
2.4	Organisation des reports	Aider les départements à traiter les reports	Communication Délais et contrôle	Tous les ans à la fin de la deuxième semaine de	0
2.5	Gestion des salaires	Aspects financiers de la gestion salariale en coopération avec la section RH Planification et contrôle des salaires	Paiement des salaires en temps utile et collaboration avec le PMO selon les nécessités	Tous les mois	0

5.3. Ressources humaines

Les activités se rapportant aux RH comprennent des tâches récurrentes et des activités générales concernant en particulier les recrutements, les évaluations de la performance, la formation, la santé et la sécurité au travail, la gestion des congés, la tenue à jour des droits individuels et la gestion des salaires. L'objectif des RH consiste à assurer le recrutement en temps utile et à suivre une politique de rétention du personnel conforme aux statuts du personnel.

En 2010, la section RH compte consolider les changements organisationnels de 2009, qui ont marqué une évolution vers un contrôle hiérarchique accru de l'Agence sur l'exécution des objectifs opérationnels au niveau des PTPA. En 2010, les priorités de la section RH englobent:

- Planification récurrente des ressources (plan définissant la politique du personnel)
- Actions positives mesurables de rétention du personnel (taux de réduction naturelle des effectifs, objectifs, coût de la rotation des effectifs, formations, promotions, etc.)
- Offre de services par gestion électronique des tâches

Les principales activités prévues pour 2010 sont les suivantes:

Réf	Détails	Livrables	Indicateurs de performance	Calendrier	Budget
3.1	Plan définissant la politique du personnel et modalités d'application	Préparer, mettre à jour et suivre tous les changements requis ou apportés aux statuts du personnel et à ses modalités d'application ainsi qu'à d'autres lignes directrices concernant le personnel, si nécessaire. Élaborer le plan définissant la politique du personnel, le mettre à jour et effectuer son suivi	Mise à jour des modalités d'exécution. Communication avec le personnel. Liaison avec le comité du personnel et les services de la Commission sur les modalités d'application et le plan définissant la politique du personnel	En continu	0
3.2	Titre 1: salaires et droits individuels Comité de classification Coûts de gestion de la CE	Établissement mensuel des salaires et des charges patronales effectué à temps. Droits individuels Comité de classification Coûts de gestion de la CE	Gestion du titre 1 et des salaires. Vérification des écritures HB. Coordination avec ACC et PMO concernant l'exactitude des écritures. Contrôle a posteriori des paiements. Coûts de gestion de la Commission européenne relatifs aux services salariaux prestés	Tous les mois. Comité de classification (2-4 sessions/an)	4 520 000
3.3	Évaluation des performances	Évaluation annuelle des performances et des périodes d'essais. Calendriers et communication. Soutien pour les recours. Suivi des descriptions de poste et de l'exécution des tâches	Nombre d'évaluations effectuées. Planification. Conclusion des procédures en temps utile	Une fois par an. Pour les périodes d'essai, selon les besoins	0
3.4	Programme de formation annuel	Programme de formation (interne, externe, sur initiative personnelle). Préparation, traitement et évaluation des formations	Planification de la formation Présentation et acceptation des documents. Programmes de formation concernant les domaines de performance clés	Tous les ans	100 000
3.5	Plan de recrutement	Exécution du plan de recrutement de l'Agence en conformité avec le tableau des effectifs. Publication d'annonces de poste. Organisation de comités de sélection. Communication avec les candidats. Mise au courant des personnes nouvellement recrutées	Nombre d'agents recrutés pour occuper de nouveaux postes ou compenser les départs. Rapidité du recrutement. Planification des conseils pour la réinstallation du personnel	En continu	474 200
3.6	Santé et sécurité au travail	Programme annuel de santé et de sécurité du personnel	Gérer le programme annuel de santé et de sécurité du personnel (examens médicaux, visites médicales avant le recrutement, conditions de travail, premiers secours, conseiller médical, centre médical)	Tous les ans	44 000
3.7	Services de tiers	Services d'intérim et de consultance	Services d'intérim pour assurer des tâches ou missions très courtes et un soutien saisonnier. Consultance dans le domaine T1, par exemple conseil juridique.	Tous les ans	159 000

5.4. TIC

La section TIC gère les principaux systèmes et réseaux internes TIC de l'Agence. Elle forme une entité à valeur ajoutée qui repose sur la réponse aux demandes des clients, et assure la planification et le bon fonctionnement de tous les systèmes à tout moment, y compris les serveurs, les bases de données, les dispositifs clients (ordinateurs de bureau, ordinateurs portables, téléphones cellulaires, etc.), les réseaux sectoriels, les communications, etc. Une partie des activités en matière de TIC est confiée à des tiers, en particulier en ce qui concerne les connexions IP, les systèmes de gestion financière etc., mais la section TIC joue un rôle de liaison et de soutien. La section TIC est le point de contact unique pour toutes les ressources informatiques disponibles; elle répond aux besoins des utilisateurs et assure les plans d'urgence et la continuité des activités. En 2010, les priorités de section TIC englobent les aspects suivants:

- Mise à jour des matériels et logiciels en bout de vie
- Niveaux de service pour la gestion électronique des tâches
- Gestion des risques en ce qui concerne la continuité des activités

En 2010, les principales activités prévues pour la section TIC sont les suivantes:

Réf.	Détails	Livrables	Indicateurs de performance	Calendrier	Budget
4.1	Planification des systèmes TIC sur les plans du matériel, des logiciels et des réseaux	Réseaux et systèmes des TIC en place gérés par L'ENISA ou une tierce partie Administration des licences de logiciels Besoins des utilisateurs	Disponibilité et intégrité des systèmes. Périodes d'inactivité. Planification de l'indisponibilité	En continu	105 000
4.2	Coûts des services TIC et ABAC	Déterminer et maintenir les niveaux de service disponibles	Mise en œuvre des services conformément à des niveaux prédéfinis	En continu	85 000
4.3	Soutien interne TIC	Gestion et soutien relatifs à ABAC. Assistance générale pour les systèmes et réseaux, et help desk. Maintenance. Exécution de tests	Demandes d'assistance. Résultats d'un plan de tests. Plan de maintenance	En continu	0
4.4	Gestion des risques et plan de sécurité pour les ressources de l'Agence Continuité des activités	Gestion de la confidentialité de l'intégrité des systèmes. Coordination avec ITMAC, la section gestion des risques et le cabinet technique	Planification et mise en œuvre des mesures d'atténuation des risques Traitement des incidents de sécurité	Tous les trois mois	0

5.5. Affaires juridiques

La section juridique se charge d'activités d'exécution du budget et de contrôle incluant la gestion générale des contrats et des marchés publics de l'Agence. Sa mission est double car elle assure la conformité de l'Agence par rapport aux dispositions juridiques et réglementations en vigueur et fournit des services à la direction et au personnel en vue de l'atteinte de leurs objectifs de mise en conformité. La section juridique fournit à l'Agence des conseils et services juridiques ainsi que des conseils et services pour les procédures de passation de marchés publics. Elle peut également remplir les tâches opérationnelles ad hoc que pourraient lui demander les départements opérationnels. En 2010, les priorités de la section juridique sont les suivantes:

- Organisation des services de back-office sur le plan de la gestion électronique des tâches pour l'administration de la passation des marchés publics
- Planification efficace des projets de passation des marchés publics
- Planification de la gestion des marchés

Les principales activités prévues pour 2010 sont les suivantes:

Réf.	Détails	Livrables	Indicateurs de performance	Calendrier	Budget
5.1	Conseil juridique en fonction des demandes du DE et des départements. Coordination de la protection des données	Avis juridiques en réponse aux demandes. Représentation de l'Agence dans toutes les circonstances appropriées. Participation au travail et à des événements internes et externes. Tâches des délégués à la protection des données et comptes rendus au CEPD	Nombre de cas traités pour l'Agence (avis juridiques, plaintes, affaires juridiques, rapports résumant les principaux éléments et partageant les informations pertinentes)	En continu	0
5.2	Marchés publics	Recours régulier à des procédures de passation de marchés publics, et prestation de l'assistance appropriée à tous les départements. Planification des achats	Plans d'achat pour l'Agence, formulaires et fiches de circulation disponibles, nombre et types de processus d'achats traités, dossiers organisés. Dossiers de bons de commande. Base de données fournisseurs. Demandes de renseignement traitées. Planification des achats et consolidation des activités d'achat	En continu	0
5.3	Gestion des contrats	Assistance générale à la gestion des contrats	Nombre de contrats préparés et signés par l'Agence, nombre de demandes d'assistance reçues des départements, nombre de réclamations reçues à ce sujet. Fiches de circulation	En continu	0
5.4	Soutien opérationnel	Fourniture d'un soutien juridique aux activités opérationnelles de l'ENISA en fonction des demandes et accords	Temps consacré à l'administration de ces opérations et à fournir des informations en retour	Ad hoc, en fonction des demandes et accords	0
5.5	Représentation	Représentation dans le cadre d'événements officiels, et représentation devant les autorités administratives et budgétaires et les tribunaux, avec l'autorisation du DE	Nombre d'affaires traitées	En continu	0

5.6. Comptabilité[13]

À l'ENISA, la comptabilité est une fonction discrète qui couvre les tâches suivantes, conformément au règlement financier:

- Comptes annuels de l'Agence
- Livres de comptes, y compris un journal, un registre général et un inventaire
- Inventaires des biens
- Paiements, etc.

Réf.	Détails	Livrables	Indicateurs de performance	Calendrier	Budget
6.1	Paiements et comptes	Exécution des paiements Comptes rendus Comptes annuels	Exactitude, réponses en temps utile, respect des délais officiels	En continu	0
6.2	Coordination des audits	Avis du comptable Conseils à la direction et au personnel concernant les questions de comptabilité. Coordination avec les parties prenantes extérieures, à savoir la Cour des comptes, selon les besoins, etc.	Nombres de cas soutenus. Réponses en temps utile	En continu	0

[13] Depuis le récent réalignement organisationnel, la comptabilité présente ses rapports au département administratif.

Résumé des activités administratives

AAD 1	Administration générale	Ligne budgétaire	Budget	Personnes-mois [14]	Nouvelle activité
AAD 1.1	Planification des activités administratives et représentation	N/A	N/A	1,6	NON
AAD 1.2	Conseil et assistance	N/A	N/A	3	NON
AAD 1.3	Niveaux d'information sur les ressources de l'Agence	N/A	N/A	2	NON
AAD 1.4	Suivi des résultats d'audit	N/A	N/A	2	NON
AAD 1.5	Tâches organisationnelles générales	N/A	N/A	13,4	NON
AAD 1.6	Services de bureau	Titre 2, sauf chapitre 23 TIC	384 000	10	NON
AAD 1.7	Contacts avec les autorités de la République hellénique et conseils à ces autorités[15]	N/A	N/A	3,2	NON
AAD 1.8	Traitement des demandes du personnel concernant la mise en œuvre de l'accord de siège (cartes ID spéciales, immatriculations de voitures, exonération de TVA, etc.).	N/A	N/A	3,2	NON
	TOTAL		**384 000**	**38,4**	
AAD 2	**Finances**	**Ligne budgétaire**	**Budget**	**Personnes-mois**	**Nouvelle activité**
AAD 2.1	Ouverture et clôture du budget annuel	N/A	N/A	3	NON
AAD 2.2	Exécution et consolidation des contrôles internes	N/A	N/A	19,2	NON
AAD 2.3	Rapports sur le budget annuel	N/A	N/A	2,6	NON
AAD 2.4	Organisation des reports	N/A	N/A	2	NON
AAD 2.5	Gestion salariale	N/A	N/A	2	NON
	TOTAL			**28,8**	
AAD 3	**Ressources humaines**	**Ligne budgétaire**	**Budget**	**Personnes-mois**	**Nouvelle activité**
AAD 3.1	Plan de politique du personnel	N/A	N/A	2	NON
AAD 3.2	Gestion salariale, droits individuels et classification	Chapitre 11	4 520 000	9,6	NON
AAD 3.3	Évaluation des performances	N/A	N/A	4,0	NON
AAD 3.4	Programme annuel de formation	1320	100 000	4	NON
AAD 3.5	Plan de recrutement	Chapitre 12	474 200	14,6	NON
AAD 3.6	Santé et sécurité au travail	1310	44 000	1	NON

[14] Une année complète correspond à 9,6 mois par membre du personnel sur l'organigramme.
[15] Cette tâche est accomplie par l'officier des ressources humaines.

AAD 3.7	Services de tiers	Chapitre 14	159 000	0	NON
	TOTAL		**5 297 200**	**38,4**	
AAD 4	**TIC**	**Ligne budgétaire**	**Budget**	**Personnes-mois**	**Nouvelle activité**
AAD 4.1	Planification des systèmes TIC	2300	105 000	4,8	NON
AAD 4.2	Services TIC	2301+2302	85 000	4,8	NON
AAD 4.3	Soutien interne TIC	N/A	0	14,4	NON
AAD 4.4	Gestion des risques informatiques et continuité des activités	N/A	0	4,8	NON
	TOTAL		**190 000**	**28,8**	
AAD 5	**Affaires juridiques et achat**	**Ligne budgétaire**	**Budget**	**Personnes-mois**	**Nouvelle activité**
AAD 5.1	Conseil juridique et représentation	N/A	N/A	6	NON
AAD 5.2	Marchés publics	N/A	N/A	9,6	NON
AAD 5.3	Gestion des contrats	N/A	N/A	2	NON
AAD 5.4	Soutien opérationnel	N/A	N/A	0,6	NON
AAD 5.5	Représentation	N/A	N/A	1	NON
	TOTAL		**0**	**19,2**	
AAD 6	**Comptabilité**	**Ligne budgétaire**	**Budget**	**Personnes-mois**	**Nouvelle activité**
AAD 6.1	Paiements et élaboration des comptes annuels	N/A	N/A	25,6	NON
AAD 6.2	Coordination des audits	N/A	N/A	À déterminer	NON
	TOTAL		**0**	**25,6**	
	TOTAL GÉNÉRAL		**5 871 200**	**179,2**	

6 ACTIVITÉS DE LA DIRECTION

À la direction de l'ENISA, les lignes de rapport garantissent la fonction horizontale de la comptabilité.

61. Relations avec les autorités de la République hellénique

Les relations avec les autorités de la République hellénique sont associées à l'obligation des parties à l'accord de siège conclu entre la République hellénique et l'ENISA. Les tâches principales de cette activité concernent la coopération et l'interaction régulières avec:

- le ministère des transports et des télécommunications, qui est le ministère compétent en matière de sécurité de l'information et le principal ministère pour toutes les questions relatives à l'ENISA;
- les entités politiques et d'administration publique en Grèce;
- le comité intraministériel établi par la République hellénique dans le but de traiter rapidement et efficacement toute question relative à l'ENISA;
- les autorités locales (préfecture, municipalité, police), pour assurer le fonctionnement sans entrave de l'Agence et la protection des droits du personnel;
- le ministère des affaires étrangères, pour la gestion des questions relatives aux privilèges attribués à l'Agence en tant que mission diplomatique ainsi qu'à son personnel (cartes d'identité spéciales, plaques d'immatriculation CD, exonérations de la TVA, etc.).

Réf.	Détails	Livrables	Indicateurs de performance	Calendrier	Budget
6.1.1	Contacts avec les autorités de la République hellénique	Contacts, rapports et suivi sur les diverses activités qui concernent les autorités de la République hellénique	Traitement de chaque cas en temps utile, respect des délais	En continu	0

Résumé des activités de la direction

DIR		Ligne budgétaire	Budget	Personnes-mois[16]	Nouvelle activité
DIR 1.1	Contacts avec les autorités de la République hellénique, fourniture de conseils à ces autorités et traitement des demandes de l'Agence relatives à la mise en œuvre de l'accord de siège.	N/A	N/A	3,2	NON
	TOTAL		**0**	**3,2**	
	TOTAL GÉNÉRAL		**0**	**3,2**	

[16] Une année complète correspond à 9,6 mois par membre du personnel sur l'organigramme.

7 ANNEXE 1 – ACTIVITÉS OPÉRATIONNELLES EN 2010

ACTIVITÉS OPÉRATION-NELLES 2010		RH opérationnelles (Note 1)	Coûts salariaux RH opérationnelles (Note 2)	Dépenses opérationnelles (Note 3)	Frais généraux (Note 4)	Coût total des activités
PTPA 1:	Améliorer la résilience des réseaux de communication électroniques européens	6,2	620 814	545 000	268 936	1 434 210
PTPA 2:	Développer et entretenir des modèles de coopération	6,3	625 707	315 000	270 512	1 211 218
PTPA 3:	Identifier les risques émergents afin d'instaurer la confiance	3,9	387 813	235 000	167 663	790 476
AP 1:	Identité, responsabilité et confiance dans l'internet du futur	1,9	187 400	0	81 018	268 418
AP 2:	Identification des moteurs et des cadres de la coopération sectorielle de l'UE en matière de SRI	1,0	101 508	105 000	43 885	250 393
AH 1:	Fourniture de conseil et d'assistance	0,0	0	0	0	0
AH 2 :	Communication et contact	7,6	759 385	174 000	328 305	1 261 690
AH 3:	Gestion des organes et groupes de l'ENISA	1,6	156 166	210 000	67 515	433 682
AH 4:	Gestion des relations avec les parties prenantes externes	0,3	27 069	428 000	11 703	466 772
AH 5:	Gestion des capacités internes de l'ENISA	0,0	0	45 000	0	45 000
AH 6:	Gestion de la communication interne à l'ENISA	0,3	26 028	0	11 253	37 280
AH 7:	Élaboration du programme de travail	0,9	92 659	0	40 059	132 718
Gestions activités sections		4,2	421 129	0	182 066	603 195
Gestions activités chef de département		0,9	93 700	0	40 509	134 209
Activités de secrétariat		6,0	599 679	0	259 259	858 938
Total		41,0	4 099 056	2 057 000	1 772 144	7 928 200

Note 1: les ressources humaines opérationnelles se composent du personnel de l'ENISA et des experts nationaux détachés participant directement aux activités opérationnelles.

Note 2: les coûts salariaux des ressources humaines opérationnelles comprennent les coûts afférents au personnel et aux experts nationaux détachés participant directement aux activités opérationnelles.

Note 3: les dépenses opérationnelles sont les coûts directs attribués à chaque activité, prévus dans le programme de travail et la déclaration de dépenses 2010.

Note 4: les frais généraux comprennent tous les coûts non opérationnels tels que les salaires du personnel non opérationnel et les frais de fonctionnement (par ex. fournitures de bureau), etc.