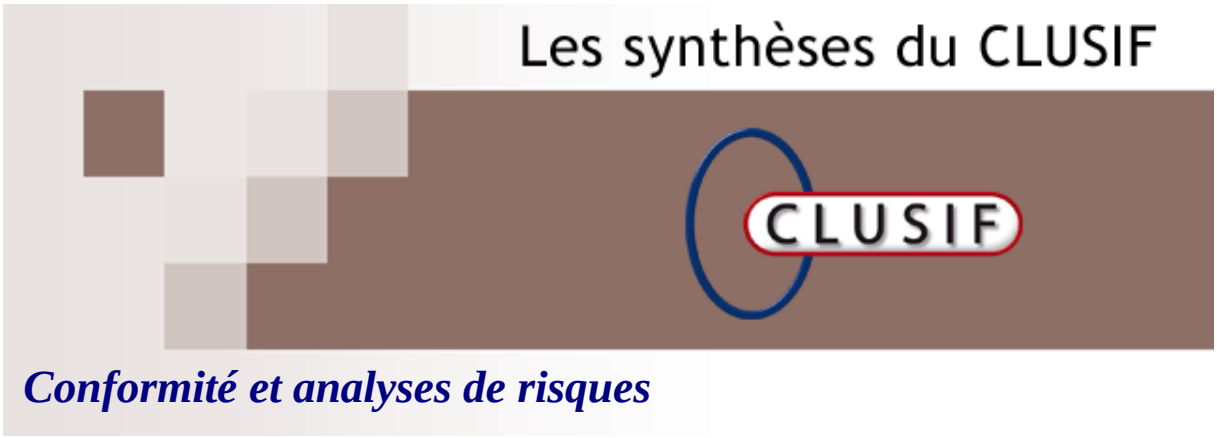

Conformité et analyses de risques

Synthèse de la conférence thématique du CLUSIF du 13 décembre 2012 à Paris

Lazaro Pejsachowicz, Président du CLUSIF, annonce qu'en cette année du 20e anniversaire du CLUSIF, Jean-Philippe Jouas, qui a beaucoup œuvré pour le CLUSIF, fera l'introduction de la conférence.

Jean-Philippe Jouas, CLUSIF

Jean-Philippe Jouas emploie le mot « maîtrise » des risques parce que « analyse » est plutôt technique et qu'il souhaite aborder plutôt le côté politique de conformité ou de maîtrise des risques.

Le sujet de la conférence revient à demander s'il faut choisir entre l'un ou l'autre.

La politique de conformité c'est la conformité à un référentiel : ISO 27001 par exemple, mais le cadre peut aussi être plus restreint, informations privées, référentiel métier, bancaire, santé etc. Celui qui choisit cette politique attend que sa conformité soit opposable à des tiers en cas d'incident et qu'elle donne confiance (aux partenaires, aux clients etc.).

Choisir une politique de maîtrise des risques c'est s'assurer qu'aucun risque n'est ignoré, sous évalué ou insuffisamment traité. Enfin, tous les risques doivent être identifiés : c'est l'enjeu d'une véritable maîtrise de risques.

Qu'on choisisse une politique ou l'autre, les conséquences sont les mêmes dans près de 80 % des cas. La raison est simple : le référentiel est par nature basé sur des bonnes pratiques qui couvrent tous les risques courants.

En revanche certains risques spécifiques peuvent ne pas être abordés par ce référentiel. Ces risques sont spécifiques parce que rattachés à un métier particulier, à une technologie particulière ou à un contexte de travail particulier. Or, une norme est par nature un compromis qui établit des règles acceptables par tous. Les risques très spécifiques pourraient bien se trouver en dehors des solutions implantées à partir de cette norme.

Par ailleurs, la norme est essentiellement une bonne pratique technique et elle risque donc d'exclure les traitements purement « métier ». Ils seront plus facilement identifiés par une politique de maitrise des risques.

Concernant les acteurs et le mode de pilotage :

La politique de conformité exige du commanditaire l'allocation de ressources et le plein support de la démarche. Par exemple, l'émergence de la norme 27001 a permis aux RSSI de se voir attribuer des moyens et en ce sens, la norme a eu un effet bénéfique. En revanche, cette politique risque de faire reposer les actions sur la seule fonction sécurité (RSSI et DSI) et permet parfois à la direction de se défausser de sa responsabilité de sécurité.

Alors que pour gérer les risques, la direction doit être fortement impliquée. C'est elle qui déclare quels risques sont inadmissibles et quels sont les risques théoriquement inadmissibles avec lesquels il faut composer quand même. La gestion des risques implique également un planning, qui implique parfois de vivre avec des risques inadmissibles pendant plusieurs années : ceci implique forcément la direction.

Concernant les objectifs :

La politique de conformité vise très clairement à propager une image et donner confiance. Autre objectif possible : avoir une ligne de défense en cas d'incident de sécurité.

L'objectif de la gestion des risques est beaucoup plus interne. C'est un outil de pilotage de la direction qui permet d'anticiper une gestion de situation de crise, de maîtriser les risques et de préparer à l'avance son discours.

Ces deux politiques sont différentes et permettent de faire un choix. Elles sont compatibles également, mais dans ce cas, une méthode de gestion des risques s'impose (Méhari par exemple).

***

Frédéric Malmartel, Agence Centrale des Organismes de Sécurité Sociale (ACOSS)

Frédéric Malmartel propose un retour d'expérience sur les actions menées par l'ACOSS.

La démarche de sécurité de l'ACOSS est basée sur le management du risque IT. Elle s'inspire de la roue PDCA (Plan-Do-Check-Act) pour s'améliorer en permanence et parvient ainsi à la conformité sur de nombreux domaines. Cette roue de Deming se trouve partout, dans la gestion du risque, dans l'analyse du risque et dans la mise en œuvre des sécurités. En tant que grande administration qui gère des fonds publics, la conformité est incontournable pour l'ACCOS, aussi bien au niveau de la loi qu'au niveau réglementaire.

A l'ACOSS, conformité et sécurité sont considérées comme complémentaires. Par exemple, se mettre en conformité avec le code des marchés est l'occasion de bien structurer les demandes en cas d'appels d'offres. C'est l'occasion de faire réfléchir les experts sur des questions auxquelles ils n'auraient pas forcément réfléchi. Il y a quelques années, la conformité était une contrainte. Aujourd'hui les experts intègrent mieux le fait qu'ils agissent dans un cadre juridique : ils sont responsables de l'utilisation des fonds publics et pour eux cette approche de la conformité a été une occasion d'améliorer leurs actions.

L'analyse de risques est basée sur une approche normative, principalement ISO 27001 mais aussi 27002. C'est à partir de cette norme ISO 27002 qu'a été construite la politique nationale de sécurité des systèmes d'information. Ce sont les comptables qui sont à l'origine de cette politique car c'est l'agent comptable qui est responsable des sécurités. Il a informé les RSSI de la nécessité de bâtir une politique de sécurité. Ces derniers ont repris certains chapitres de la norme ISO 27002, les ont retravaillé et ont bâti une politique nationale de sécurité. Elle est améliorée chaque année, complétée notamment par des audits décidés en interne ou des audits de la Cour des comptes par exemple.

Aujourd'hui, un contrôle supplémentaire consiste à reprendre la norme ISO 27002 afin de vérifier sur quels points elle est respectée ou non. La norme ISO 27002, dans son dernier chapitre, traite de la conformité aux lois et aux règlements. C'est aussi une occasion de réfléchir à nouveau sur la sécurité.

Mais cette approche ne supprime pas les impondérables. Lors du lancement de la politique nationale de sécurité, les contraintes étaient nombreuses : un réseau de 14 000 personnes, 105 Urssaf, 7 centres informatiques. L'approche normative a été une aide et elle l'est toujours face aux exigences de conformité. Il faut savoir aussi que cette politique nationale de sécurité a été mise en place pour répondre à une contrainte : la validation des comptes. C'est donc une contrainte de conformité qui a été à l'origine de l'élaboration de la politique de sécurité.

Les audits ne sont plus considérés comme une contrainte et ils sont l'occasion de bâtir des éléments qui aident à la mise en conformité. Dans ce sens, afin de mieux répondre aux exigences de la CNIL, les responsables CIL ont créé une cellule nationale, portée par la Direction.

L'exigence de conformité :

- apporte la possibilité d'évaluer les exigences en fonction de critères de qualité,
- permet de prendre du recul par rapport aux demandes en matière de conformité, (la conformité n'étant pas un objectif en soi, qui doit faire oublier le métier de l'ACOSS),
- offre la possibilité d'avoir un langage commun, avec le RGS par exemple,
- permet de structurer la démarche en matière d'analyse de risques, grâce à des niveaux d'exigence élevés : ceux du RGS ou de la CNIL par exemple.

Pour envisager de faire coexister la conformité et l'analyse de risques, l'implication de la Direction s'avère nécessaire. Cette condition est respectée au sein de l'ACOSS, tout particulièrement depuis l'obligation de faire certifier les comptes.

Les questions suivantes se posent :

- La non-conformité présente-t-elle un risque particulier ?
- Faut-il la prendre en compte dans l'analyse de risques ?

Pour l'ACOSS, la non-conformité n'est pas un risque particulier, c'est un risque comme les autres, (incendie, dégât des eaux etc.). La mise en œuvre d'une application ou d'un projet nouveau génère un certain nombre de risques (erreur, piratage etc.) dont celui d'être non conforme. A l'ACOSS ce risque est inadmissible et à ce titre il est traité pour qu'il disparaisse.

L'ACOSS a mené ses analyses de risque avec différents outils (Marion, EBIOS) ainsi qu'avec des outils « maison ». Si la norme 27005 est claire, des réserves peuvent être émises sur ces méthodes d'analyse de risque, bien conçues par les experts mais souvent complexes.

Pour bénéficier d'une gestion dynamique de la conformité, il faut être réactif et savoir partager la connaissance. L'ACOSS tente également d'avoir un système d'information qui permette d'anticiper la conformité afin d'être prête en cas de nouvelle réglementation européenne par exemple.

Une piste de réflexion possible serait d'inscrire l'analyse de risque, puis la gestion des risques, dans une démarche ITIL : la mise en conformité deviendrait alors perpétuelle.

***

Baptiste Parent, Caisse Nationale d'Assurance Maladie (CNAMTS)

Baptiste Parent souhaite aborder le sujet sous un nouvel angle : il considère que l'analyse de risque peut intervenir au secours de la conformité et inversement.

La question est de savoir comment proposer une gouvernance des risques IT cohérente en prenant en compte les contraintes qui pèsent sur les projets SSI, les directives ou politiques de SSI :

- contraintes externes : réglementaires (du point de vue législatif ou de la conformité), ou liés aux contrôles et audits ;
- contraintes internes : politiques internes, audits internes, analyse de risque.

La position de la CNAMTS est illustrée par les travaux qu'elle a réalisés cette année dans le cadre de la mise en œuvre de sa nouvelle politique de systèmes d'information. Elle a d'abord tenté la mise en place de la roue Deming PDCA mais l'a supprimée devant les difficultés qui se sont présentées. Elle a essayé ensuite de progresser dans une démarche SMSI, non sans mal.

Le constat s'est imposé que le choix de la méthode n'était pas le bon, que l'analyse de risques choisie n'était pas adaptée à l'Assurance maladie.

En effet, l'objectif de cette PSSI était de bâtir une politique de sécurité SI globale pour toute l'entreprise. Or, l'Assurance maladie est un réseau d'organismes très hétérogènes qui connaissent chacun leurs risques propres.

L'analyse de risques devait donc être basée sur :

- Une analyse de risque spécifique couvrant un large spectre de risques : métiers, organisationnels, techniques et réglementaires.

- Le besoin de conformité imposé par les autorités de tutelles, notamment la Cour des comptes.

La PSSI s'est faite en trois phases :

1. Analyse des risques.
2. Rédaction de la PSSI.
3. Constitution du plan de traitement des risques.

L'analyse de risques, orientée processus métier, est basée sur EBIOS. Elle aboutit à une cartographie des risques par type d'organisme. Une fois cette cartographie établie, le travail s'est fait en trois phases également :

1. Identification des moyens de couverture des risques déjà en place.
2. Identification des mesures ISO27002 concernées par les risques.
3. Rédaction des préconisations de la PSSI.

Ces trois phases réalisées, le problème reste la prise en compte des besoins de conformité. La Cour des comptes par exemple, dit que la politique de sécurité d'un organisme public, doit être conforme à l'ensemble des mesures présentes dans l'ISO 27002.

Or, la CNAMTS constate que sa Déclaration d'Applicabilité retient 75 % des mesures détaillées dans la norme ISO 27002. Afin d'atteindre l'objectif de 100 %, elle crée un « risque général » dont le traitement nécessite la mise œuvre des 25 % restantes.

Malgré un périmètre de couverture qui n'était pas exhaustif, la déclaration d'Applicabilité couvrait l'ensemble des chapitres de l'ISO27002. La non-couverture des 25 % restants pouvait avoir pour cause :

- la non-exposition au risque concerné par la mesure,
- la non-identification d'un risque au cours de l'analyse,
- une erreur dans la mise en correspondance réalisée entre les risques et les mesures ISO27002.

La question qui se pose naturellement est :

Pourquoi continuer à réaliser une analyse de risques si finalement la totalité des 133 mesures de la norme ISO 27002 doivent être retenues ?

Ce « risque général » a été crée pour satisfaire le besoin de l'auditeur : s'assurer que l'ensemble des mesures de la norme sont couvertes. Mais la CNAMTS souhaite continuer à mener des analyses de risque pour leur apport de la connaissance des risques et du traitement associé. Cette connaissance des risques et de leur traitement se matérialise dans la rédaction des préconisations détaillées.

Cette rédaction s'établit à partir de deux « inputs » :

- La prise en compte des dispositifs de sécurité déjà présents et opérationnels.
- Les résultats de l'analyse de risques qui nous permettent d'être assurés que les préconisations couvriront les risques identifiés.

Les mesures que l'on aura raccrochées pour les besoins de conformité bénéficient de préconisations plus légères, en raison de leur faible exposition aux risques. Il peut arriver aussi que la CNAMTS considère que le sujet est déjà traité et dans ce cas, aucun dispositif opérationnel ne sera mis en œuvre.

****

Olivier Corbier, Docapost

Les principaux référentiels utilisés par Docapost sont :

<u>Des Référentiels métiers</u> :

- Le label FNTC-TA, dédié au service de tiers archivage,
- GS1 (échanges électroniques, EDI),
- RGS,
- les recommandations CNIL concernant le vote électronique.

<u>Des normes ou obligations réglementaires sectorielles</u> :

- Le Code général des impôts pour la dématérialisation fiscale,
- le CCRLF 97/02 pour tout ce qui concerne les banques,
- PCI-DSS.

<u>Des activités certifiées</u> :

- Certification ISO 9001 sur l'ensemble des activités industrielles.
- Certification ISO 27001 sur la partie archivage électronique.

Des démarches transverses au groupe Docapost ou au groupe La Poste :

- Certification ISO 14001 pour l'environnement.
- Certification ISO 26000 pour la responsabilité sociétale.

Toutes ces fonctionnalités sont essentielles aux offres Docapost.

S'ajoutent des conformités techniques plus ou moins obligatoires, le référencement de l'Autorité de certification par les navigateurs par exemple.

Docapost répond également à la nécessité, plus « marketing » d'assurer une veille technologique et réglementaire. L'entreprise a un devoir de conseil auprès de ses clients sur la législation qui évolue régulièrement.

La multitude de référentiels applicables entraîne de vrais risques de non conformités. Par exemple :

- Les engagements de conformité sont inscrits dans les contrats et en cas de non-conformité, Docapost s'expose à une interdiction d'exercer les métiers concernés.
- L'Obsolescence technologique ou juridique sur les activités d'archivage électronique par exemple peut entraîner la nécessité d'un volume très important et soudain de migrations.

La conformité chez Docapost bénéficie d'une implication très forte de la Direction qui s'appuie sur un département QSE (Qualité, Sécurité, Environnement) constitué d'experts qualités et d'auditeurs internes. Ils gèrent les audits, managent les certifications 9001 et les traduisent en processus opérationnels. Les risques de non-conformité sont remontés au niveau stratégique.

Mais les activités de Docapost sont très cloisonnées et la conformité contribue souvent à renforcer ce cloisonnement. En effet, lorsque des processus ont été mis en conformité, ils ont tendance à se figer : la conformité est une excuse pour ne « plus bouger ». Or, Docapost étant aussi un groupe qui propose des activités transverses, il est nécessaire que ces activités soient interconnectées.

Par ailleurs, les référentiels étant par définition figés, même très complets, ils ne peuvent prétendre à l'exhaustivité. Or, la composante IT est très forte chez Docapost (peu d'externalisation, importante offre de services sur internet etc.). La conformité est concentrée sur l'offre mais ne règle pas toutes les préoccupations en sécurité des SI.

Le rôle du RSSI :

Dans un contexte où :

- l'organisation interne fait l'objet de changements fréquents (fusions, regroupements ou créations d'activité),
- les obligations de conformité sont multiples,

➢ Il veille à ce que la conformité soit préservée, lors des échanges et des opérations communes entre services qui ne répondent pas forcément aux mêmes normes.

➢ Il gère les projets d'optimisation : Docapost est un groupe jeune, crée en 2008, qui a besoin d'homogénéiser ses pratiques, ses compétences et ses référentiels.

Une démarche en sécurité de l'information du groupe implique par conséquent :

- Une cohérence et une cohésion entre les différentes activités.
- Une démarche d'amélioration continue, notamment dans la gestion des changements.
- Des processus SSI transverses (outillage technique, cartographie et classification, expertise technique).

Le groupe doit donc se doter :

- d'un SMSI décliné selon les périmètres et consolidé au niveau groupe. L'idée étant de consolider au niveau groupe les indicateurs, les tableaux de bord etc. et que tout le monde parle le même langage ;
- d'un outillage complet en management des risques : analyse de risques complète, risques individualisés et risques projet.

La conformité donne des leviers très importants au RSSI :

- L'implication de la Direction.
- L'inscription dans une gouvernance :
  - des ressources disponibles (département QSE, service juridique),
  - de la définition et formalisation des responsabilités,
  - des formalismes existants (enregistrement au sens 9001).
- La matérialisation du travail accompli (labels, certificats), fort vecteur de motivation des équipes.
- Des échéances qui remettent les projets SSI dans la liste des actions prioritaires.
- Des référentiels de conformité qui commencent à parler d'analyse de risques (PCIDSS, 27001 etc.).

Pour gérer les risques et la conformité il faut :

- Se doter d'un modèle de risque « référent » (pouvant être réutilisé, quelque soit le rapport d'audit réalisé),
  - qui soit consistant, rationnel, rigoureux, intelligible,
  - dont les concepts et la terminologie sont bien décrits,
  - qui détermine les automatismes, les grilles de décision,
  - doté de tables de références minimales qui évoluent.
- Documenter les correspondances, les équivalences et les différences terminologiques avec les autres référentiels.
- Décliner ce modèle dans les processus (dans le sens des activités ITIL), par exemple :
  - constitution et suivi des plans d'action,
  - gestion des incidents et des problèmes,
  - classification des informations,
  - cadrage des projets,
  - monitoring et indicateur.

Ce modèle ne doit pas pour autant être :

- trop précis : les précisions seront apportées là où elles sont nécessaires et il doit réussir à englober les modèles et concepts proches,
- trop rigide : il doit pouvoir évoluer au gré des nouvelles versions de référentiels, ou au gré des évolutions du contexte. Il faut garder à l'esprit que c'est un outil.

Ce modèle permet :

- d'intégrer les résultats d'audit directement dans une gestion cohérente. Il est en effet dommage d'enterrer les audits une fois qu'ils ont rempli leur mission,
- de produire des tableaux de bord cohérents et consolidés,
- de communiquer sur les risques plus facilement, avec des collaborateurs formés sur le modèle,
- de faire de l'analyse de risque et donc de sécuriser le SI !

Pour conclure, gérer la conformité et gérer la sécurité de l'information sont deux choses différentes. Mais ces deux démarches sont complémentaires et doivent coexister.

Le RSSI doit rester pragmatique et ne doit pas se priver des leviers offerts par la conformité. Mais le management des risques est le seul moyen de gérer correctement la SSI. C'est aussi un outil pour soutenir le management de la conformité. Il doit dans ce cas s'appuyer sur un modèle robuste, parfaitement compris et expliqué.

****

Matthieu Grall, CNIL

Après les interventions précédentes, Matthieu Grall souhaite apporter un autre point de vue.

La CNIL, c'est avant tout 17 commissaires qui se réunissent chaque semaine pour prendre des décisions : ils font de la gestion de risques en permanence. Quand un organisme demande l'autorisation de mettre en œuvre un traitement de données à caractère personnel, ce sont eux qui en décident.

Les principales missions de la CNIL se partage en deux grandes activités :

- en amont, conseiller et évaluer la conformité ;
- en aval, contrôler et le cas échéant sanctionner.

Pourquoi gérer les risques sur les libertés et la vie privée ? Pour éviter les sanctions bien sûr. Mais surtout, l'existence d'une loi sur la protection de la vie privée est souvent un bon argument pour faire avancer les choses dans le domaine de la sécurité en général. La loi « informatique et libertés » peut en effet servir de levier pour justifier certaines actions de sécurité.

L'article 34 de loi dit, en résumé, qu'il faut déterminer des mesures proportionnées aux risques. Comment démontre-t-on qu'on est conforme à cet article ?

De manière générale, il s'agit de mettre en œuvre, pour tous les traitements de données à caractère personnel, des processus qui protègent les personnes concernées et leur permettent d'exercer leurs droits.

Certains risques portent d'ailleurs sur le fait que ces processus peuvent ne pas être mis en œuvre ou être détournés.

La loi pourrait devenir encore plus explicite en termes de gestion des risques, notamment si le prochain règlement européen sur la protection des données impose de réaliser une appréciation des impacts sur la vie privée.

La sécurité des systèmes d'information est-elle comprise dans la protection de la vie privée ou la vie privée est-elle comprise dans la sécurité des systèmes d'information ? C'est une simple question de point de vue.

En synthèse,

- la sécurité des systèmes d'information consiste à protéger l'organisme. Le RSSI regarde toutes les informations manipulées au sein de l'organisme et étudie les impacts financiers, d'image et juridiques. C'est dans ce cadre qu'il va considérer les risques de non-conformité à la loi « informatique et libertés ».
- La protection de la vie privée protège les personnes concernées des traitements mis en place par l'organisme. Le point de vue n'est pas le même que pour la SSI, et pourtant cette démarche peut être intégrée dans l'approche risque.

Si la CNIL veille à la protection de la vie privée, elle estime aussi que c'est de la responsabilité de chacun. Elle a donc formalisé des processus, de façon à les rendre le plus accessibles possible (la CNIL est essentiellement composée, non pas de spécialistes en sécurité, mais de juristes). Elle a publié deux guides :

- une méthode, qui explique comment gérer les risques sur la vie privée ;
- un catalogue de mesures, dans lequel il est possible de choisir et d'adapter des solutions pour traiter les risques encourus. Ce catalogue ne doit surtout pas servir à faire des audits de conformité !

Ces deux guides sont disponibles sur le site de la CNIL (http://www.cnil.fr/en-savoir-plus/guides/).

Selon la CNIL, un risque est un scénario décrivant un événement redouté et toutes les menaces qui le rendent possible.

- Sur la partie « menaces », les approches de la protection de la vie privée et SSI sont très communes. La partie « menace » comprend toutes les sources de risques qu'elles soient humaines ou non, internes ou externes, volontaires ou accidentelles. Même si ce sont des données à caractère personnel, il s'agit bien, aussi, « d'informations », ce qui permet aux deux approches d'être similaires.
- Sur la partie « évènements redoutés », on ne trouve que les données à caractère personnel et on considère uniquement les impacts sur les personnes.

Le principe de la méthode ressemble à toute analyse de risque. En synthèse :

1. Étude du contexte.
2. Étude des évènements redoutés : quels sont notamment les impacts sur les personnes concernées ?
3. Étude des menaces.
4. Étude des risques.
5. Étude des mesures. Elle consiste à piocher dans un catalogue de mesures comme celui proposé par la CNIL ou un autre. Et les adapter à ses risques propres.

Dans l'étude du contexte, une notion importante concerne les enjeux du système : par exemple, il faut parfois mettre en équilibre la sauvegarde des données à caractère personnel et la survie de la personne concernée. Les commissaires de la CNIL sont parfois amenés à trancher en prenant compte de ces enjeux. Et en général tout le monde y veille, intuitivement.

Pour conclure, le principe le plus important est d'apprécier les risques et de les traiter à leur juste valeur. Être souple est aussi une notion de bon sens. La méthodologie publiée par la CNIL respecte simplement une logique : c'est une démarche pour « penser » protection des personnes concernées.

Questions et Réponses avec l'assistance.

Cette conférence comportait également un débat avec la salle, non retranscrit dans ce document mais disponible en vidéo, sur le site web du CLUSIF, à l'adresse suivante : http://www.clusif.fr/fr/production/videos/#video121213.

Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF http://www.clusif.fr/fr/infos/event/#conf121213.