

# De l'élaboration d'une PSSI d'unité de recherche à la PSSI d'établissement

## Sylvie Vottier

Université de Bourgogne  
Esplanade Erasme  
BP 27877  
21078 Dijon Cedex

## Alain Tabard

Université de Bourgogne  
Esplanade Erasme / ICMUB (UMR CNRS 6302)  
BP 27877  
21078 Dijon Cedex

## Résumé

*L'Université de Bourgogne considère la sécurité de l'information comme l'un des enjeux majeurs pour l'établissement. En créant en avril 2013 le poste de RMSI (Responsable du Management de la Sécurité de l'Information), l'établissement a démontré sa volonté de développer une culture de la sécurité de l'information. Ses missions principales sont d'assurer la cohérence et le management de la sécurité de l'information de l'université en relation avec l'ensemble des services de l'établissement, de mettre l'université en conformité au Référentiel Général de Sécurité et d'assurer la PPST (Protection du Potentiel Scientifique et Technique).*

*Cette nouvelle fonction est née de la mise en place de deux PSSI dans deux unités à « Régime Restrictif » du CNRS sur le périmètre de l'université. La mission PSSI a été menée par la RMSI à travers une appréciation des risques encourus par l'information matérielle et immatérielle présente. Cette démarche participative a permis de sensibiliser fortement les acteurs, de créer un comité Sécurité des Systèmes d'Information de suivi dans chaque unité. L'analyse des risques a mis en lumière les flux d'informations sensibles existants en interne à l'université, mais aussi à l'externe vers les startups, les pôles de compétitivité ou de valorisation. L'idée est de suivre le flux de l'information sensible et d'effectuer une appréciation des risques sur chaque périmètre. Les résultats obtenus, les traitements choisis pour réduire, accepter, externaliser ou refuser les risques concourront à l'élaboration de la PSSI de l'université de Bourgogne en tenant compte de ses spécificités.*

*La RMSI anime et s'appuie sur un réseau d'une quarantaine de Chargés de Sécurité des Systèmes d'Information nommés officiellement. Ces CSSI constituent des relais de terrain indispensables. Ils sont les acteurs privilégiés des actions préventives et correctives des incidents et de leur remontée, de la sensibilisation et du développement de la culture de la sécurité de l'information sur leur périmètre. Le profil des CSSI est en cours d'évolution afin que l'ensemble des métiers présents sur l'université soit représenté.*

## Mots-clefs

*PSSI, ISO 27001, CSSI, GRI, Sécurité, Information, Sensibilisation, Risques, PPST, RMSI, ITIL, Responsabilité, externalisation, Contrat, Service, SMSI, Qualité, Système, SSI, ADAC*

## 1 Introduction

L'Université de Bourgogne a décidé de mettre l'accent sur la sécurité de l'information en créant un « Bureau de la Sécurité de l'Information ». Ce bureau, créé en ce début d'année 2013 et mis en place par un RMSI (Responsable du Management de la Sécurité de l'Information), doit assurer la cohérence et le management de la sécurité de l'information de l'établissement en relation avec l'ensemble des services de l'établissement impactés par la sécurité de l'information. L'information considérée est l'information matérielle et immatérielle présente dans les entités de l'établissement.

Cette nouvelle fonction de RMSI est née de la mise en place de deux Politiques de Sécurité des Systèmes d'information dans deux établissements à « Régime Restrictif » du CNRS sur le périmètre de l'établissement universitaire. La mission PSSI a été menée par la RMSI aujourd'hui en place, à travers une démarche d'implémentation d'un Système de Management de la Sécurité de l'Information ISO2700x et d'une appréciation des risques encourus par l'information matérielle et immatérielle présente dans les deux unités de recherche ultra sensibles au regard de l'intelligence économique, de la défense, de la prolifération et du terrorisme.

## 1.1 L'information sensible

L'information sensible représente les dossiers de stratégie ou de pilotage de l'établissement, les contrats de recherche, les dossiers de coopérations institutionnels et industriels, nationaux et internationaux, les données de recherche, les plans de bâtiments, les schémas d'infrastructures réseaux, ou les documents nominatifs tels que les cartes d'identités, visas ou contrats de travail. Ces données sensibles sont autant de données confidentielles.

De telles informations sont qualifiées d'informations « sensibles » et ont fait l'objet d'une recommandation du premier ministre le 2 mars 1994. Elles comprennent en particulier les données à caractère personnel au sens de la loi informatique et libertés ; les informations vitales pour l'exercice de la mission de l'organisme ; les informations qui sont soumises à l'obligation de réserve ou de discrétion professionnelle ; les informations constitutives du potentiel scientifique, industriel et technologique et les enjeux de la PPST (Protection du Potentiel Scientifique et Technique).

L'information matérielle représente l'information que l'on conserve sous forme papier dans les armoires, sur les bureaux ou sous forme d'archives. Il peut s'agir des contrats, brevets, dossiers de recrutement, justificatifs de mission, budget, finance, dossiers d'expertise... Elle regroupe aussi les cahiers de laboratoire qui aujourd'hui sont les seules preuves tangibles de l'antériorité d'une recherche. Le rangement au quotidien et l'archivage de ces cahiers est essentiel. Il en va de même pour les échantillons de recherche qui constituent des biens précieux aux yeux des chercheurs et qui, mis dans les mains de concurrents, peuvent dévoiler des procédés de fabrication non encore brevetés.

L'information immatérielle revient à l'équivalent électronique de l'information matérielle, les informations électroniques, les équipements informatiques, scientifiques, les contrôles d'accès physiques, mais c'est aussi l'information détenue par les individus eux-mêmes. Ceux-ci peuvent, au détour de conversation, divulguer des informations sensibles, des secrets. D'autres, par leurs mauvaises pratiques métiers, peuvent mettre en danger les informations qu'ils détiennent. Un autre risque engendré par une personne est le fait qu'elle soit la seule à avoir développé une compétence spécifique. Si cette personne quitte l'unité, c'est son savoir et donc les informations qu'elle détenait qui sont perdues, d'où le besoin de transfert de compétences.

## 1.2 Les accès

Dans ces laboratoires sensibles, des ZRR (zones à régimes restrictifs) ont été définies. L'accès à ces zones est régi par la stratégie de déploiement de la PPST du Ministère de l'Enseignement Supérieur et de la Recherche, qu'il s'agisse d'accès physique ou virtuel à des ressources de l'unité de recherche, ceci dans un cadre légal. La procédure est décrite dans la circulaire du Premier Ministre N°3415/SGDSN/AIST/PPST du 7 novembre 2012 et dans les notes thématiques PPST d'avril et juin 2013 associées.

Dans de telles unités de recherche, le contrôle d'accès aux ZRR doit se faire en entrée comme en sortie et être tracé, ceci quel que soit le type d'outils, badge, carte magnétique ou carte multiservice et quel que soit le statut des personnes : personnels privés, publics, étudiants, permanents ou temporaires ou même des sociétés de maintenance.

## 1.3 La population sensible

La population directement concernée par la Politique de Sécurité de l'Information est l'ensemble des personnels permanents et non permanents d'une unité de recherche, ainsi que les visiteurs, les étudiants, les stagiaires, les sociétés de maintenance et de surveillance du bâtiment, les personnels d'hygiène et de sécurité. S'ajoutent à cette population, les personnes provenant de coopérations ou de collaborations scientifiques.

Les coopérations scientifiques entre établissements français et étrangers conduisent à de nombreux échanges et déplacements de personnes dans les unités de recherche en France et à l'étranger. Les collaborations entre industriels et institutionnels sont de plus en plus fréquentes et induisent des échanges au sein même des unités de recherche. Ces collaborations contribuent à la valorisation de la recherche et l'on ne compte plus les naissances de startups, spin-off et

plateformes technologiques adossées aux laboratoires de recherche. Ces sociétés en devenir partagent un temps les ressources humaines et techniques des unités de recherche. Ces ressources mutualisées constituent des risques à évaluer.

## 1.4 Vers la PSSI d'unité de recherche

La maîtrise des risques sur le système d'information d'un établissement repose sur la connaissance de l'ensemble des biens à protéger, des acteurs présents sur le périmètre d'action, de l'environnement de travail. Les informations sensibles comme les acteurs sont de diverses origines, chacun ayant des enjeux différents. Et quand « tout ce petit monde » partage les mêmes ressources, difficile de cloisonner et d'assurer la sécurité des informations sensibles sans avoir une politique définie, suivie par tous et en complète harmonie avec l'exercice des métiers de la recherche, de la formation et de l'administration.

L'idée première est de s'intéresser aux informations sensibles, matérielles et immatérielles, manipulées au quotidien par les différents acteurs au cours de leur métier. L'idée suivante est de suivre le flux de l'information sensible au cours de son cycle de vie. Nous verrons que cette information sort du périmètre initial qu'est l'unité de recherche et va dans des composantes et les services centraux de l'université. Cette information sensible peut également sortir vers les tutelles institutionnelles, régionales ou nationales. D'autres informations vont vers le monde du privé et prennent le chemin des industries, des startups, des plateformes technologiques, des SATT ...

## 2 Elaboration de deux PSSI dans deux unités très sensibles du CNRS

La Délégation Régionale Centre-Est du CNRS a engagé un chargé de mission « Politique de Sécurité des Systèmes d'Information » pour effectuer une appréciation des risques encourus par l'information sensible dans deux unités de recherche très sensibles de sa région. Cette mission a été menée par la Responsable du Management de la Sécurité de l'Information recrutée aujourd'hui à l'université de Bourgogne. La RMSI a mis en place une démarche ISO27001 d'analyse des risques qui a conduit à l'élaboration d'une Politique de Sécurité de l'Information opérationnelle d'unité sur chacun des deux sites. Un plan de traitement des risques a été établi à court et moyen terme pour accompagner les directeurs d'unité dans les actions correctives et préventives nécessaires à la protection de leur potentiel scientifique et technique. Un suivi est aujourd'hui réalisé par le comité SSI constitué lors de la mission. Ce comité a un rôle de sensibilisation, de veille et assure une amélioration continue du système de management de la qualité mis en place.

### 2.1 Intérêts de la démarche ISO27001

La démarche ISO27001 menée au sein des deux laboratoires est une démarche orientée « métiers ». Tous les métiers présents dans l'unité de recherche ont été audités avec une priorité donnée aux métiers de la recherche, de la formation, de l'administration et aux métiers supports à la recherche.

La RMSI a insisté sur l'aspect fortement participatif de cette démarche. L'idée essentielle est qu'en ciblant et en impliquant les personnes métiers, une sensibilisation forte devait découler de cette démarche contribuant ainsi au développement d'une culture de la sécurité de l'information sur chacun des périmètres. La maturité de l'organisation en matière de Sécurité des Systèmes d'Information s'en trouve ainsi augmentée.

En dehors de l'approche processus métier, l'intérêt de la démarche est qu'il s'agit d'un pilotage de la sécurité par les risques. La RMSI a considéré que seuls les acteurs directement concernés pouvaient évaluer les risques en termes de confidentialité, d'intégrité et de disponibilité pesant sur les systèmes d'information qu'ils manipulent au quotidien dans le cadre de leur métier.

La politique de sécurité de l'information qui découle de cette démarche est véritablement l'œuvre de tous sur l'unité concernée. Cette politique représente l'image du Système d'Information de l'organisation à un instant t. Elle est réaliste et pédagogique et sera améliorée d'année en année grâce à la veille et au contrôle assurés par le comité Sécurité des Systèmes d'Information mis en place au cours de cette démarche.

### 2.2 Etude de contexte

Les unités de recherche concernées sont des unités de 150 à 300 personnes environ. Elles sont hébergées dans des bâtiments universitaires sur plusieurs sites territoriaux de la région Bourgogne. Chaque unité collabore avec des filiales de valorisation de la recherche ou avec des pôles de compétitivités. Ces laboratoires ont des startups ou plusieurs projets en incubation qui partagent les ressources propres humaines et matérielles de l'unité de recherche.

La population présente est un savant mélange de secteurs privé et public, de coopérations avec des pays étrangers et à risques, et de collaborations avec le monde industriel. La protection du potentiel scientifique et technique représente donc un axe majeur de prévention des risques sur ces périmètres ; risques liés à la sécurité économique, à la prolifération, au terrorisme ou à la défense.

Les bâtiments occupés aujourd'hui par ses unités de recherche n'ont absolument pas été prévus pour cloisonner facilement les différents métiers d'enseignement, de recherche et d'administration ou pour limiter les accès physiques. Les salles d'enseignement cohabitent avec les plateformes technologiques de valorisation. Les sujets de recherche brevetables partagent leur espace avec les allers et venues des étudiants. Sans caricature, ces bâtiments d'un certain âge n'ont pas été pensés « valorisation de la recherche », pôle de compétitivités, startups ...

Les choses changent fort heureusement et le paysage de la recherche voit apparaître de plus en plus de complexes scientifiques dédiés à la valorisation. En attendant, il faut déployer de l'énergie, de l'argent et faire preuve de créativité pour protéger son patrimoine scientifique. Des restructurations de ses anciens locaux sont en cours. Cette étude a permis à l'université de travailler à la protection de ce patrimoine local.

## 2.3 Mise en place de la démarche

La mission de Politique de Sécurité des Systèmes d'Information a été initiée par la Délégation Régionale Centre-Est. Une présentation de la démarche a eu lieu avec la gouvernance de chaque unité afin de décrire la conduite de projet, coordonner les différentes étapes, définir les types d'acteurs à auditer et constituer un comité Sécurité des Systèmes d'Information local, capable de faire le liant entre les actions du chargé de mission PSSI et l'ensemble des personnels, pendant la durée de la mission et après, ceci dans un but d'amélioration continue.

A l'issue de cette présentation, le directeur d'unité a élaboré un plan de communication au sein de son laboratoire de manière à ce que la chargée de mission puisse opérer plus facilement et dérouler sa conduite d'entretien auprès des personnels. La constitution du comité SSI a été engagée par le directeur d'unité et enrichie au cours de la mission.

Le périmètre de la démarche a été l'ensemble du laboratoire, y compris les sites territoriaux. Ce périmètre a été visité entièrement de manière à s'imprégner du terrain. En revanche, les personnes interviewées ont été ciblées sur les équipes qui collaborent avec des industriels ou des institutionnels sensibles ou qui détiennent et portent des brevets.

L'identification des informations sensibles s'est faite non seulement au cours d'une visite sur le terrain de l'ensemble du périmètre de l'unité, mais aussi lors d'entretiens individuels.

## 2.4 Visite de terrain

La visite de terrain s'est déroulée avec les plans de laboratoire, entretien avec les personnes rencontrées, repérage de la gestion des accès physiques, de la gestion des rangements bureaux, armoires, archives, des ressources matérielles à protéger, des ressources logicielles évoquées, de la gestion des courriers papiers, des colis ...

Les zones privilégiées ont été les bureaux administratifs, les bureaux des responsables d'équipes, les bureaux des porteurs de projets scientifiques avec des industriels ou des institutionnels ayant un niveau d'exigence important en matière de sécurité de l'information.

Les plans et visites ont permis de constater le partage de l'espace physique entre expériences scientifiques, enseignements et startup. Les bureaux communs à plusieurs personnels dont l'un est porteur de brevets et l'autre, est responsable de filière et reçoit beaucoup d'étudiants.

Très vite, il est facile de repérer ces incohérences ou le « mélange des genres » dans les usages de salles d'expériences mutualisées avec les enseignements de master, une plateforme technologique, des industriels ... Ou encore des accès physiques restreints en apparence avec badge en entrée, mais avec accès libre à l'autre bout du même bâtiment.

## 2.5 Conduite d'entretien

La conduite d'entretien s'est faite sur un échantillon de 12% du personnel dans chaque unité de recherche, en ciblant les différents métiers présents sur le périmètre et en choisissant les personnes porteuses de projets de collaborations scientifiques brevetables ou avec des industriels ou institutionnels sensibles français et étrangers.

En choisissant un petit échantillon d'interviewés sur un périmètre large, on choisit de focaliser sur les données *a priori* les plus sensibles du laboratoire et d'avoir une vue systémique des risques avec un niveau de granularité important.

La chargée de mission a élaboré une grille d'entretien à destination des chercheurs, des administratifs ou des équipes supports. Chaque entretien a été réalisé sur une durée maximale de 55 minutes. Les questionnements ont été menés suivant la méthodologie ADAC, Analyse De l'Activité et des Compétences. Cette méthodologie, déposée à l'INPI, a été développée par l'Institut du Management par les Compétences et Validation des Acquis, du Conservatoire National des Arts et Métiers. Cette méthode procède de trois démarches complémentaires :

- inventaire des activités et sous-activités mises en œuvre par la personne dans l'exercice de son métier ;
- l'inférence des savoirs à partir des sous-activités identifiées et leur classement en quatre catégories : les savoirs théoriques, les savoirs procéduraux, les savoirs de l'expérience et les savoirs pratiques ;
- la validation par les personnes interviewées des synthèses descriptives des activités et des compétences identifiées.

## 2.6 Appréciations des risques

L'intérêt de la méthode ADAC pour la démarche d'appréciations des risques est que chaque métier sera décliné en activités puis chaque activité en sous-activités. Pour chacune de ses sous-activités, il sera possible de dégager quelles sont les informations sensibles manipulées au quotidien.

En élaborant le tableau d'appréciation des risques de cette manière, les informations sensibles liées à chaque sous-activité sont mises en lumière. Il est alors possible de transcrire, pour chacune de ces informations sensibles, les menaces et les vulnérabilités que la chargée de mission aura décelées au cours de l'entretien ou de sa visite de terrain. Une fois que ces menaces et vulnérabilités sont décrites, la démarche participative énoncée plus haut consiste à donner ce tableau d'appréciation des risques à remplir aux chercheurs et administratifs interviewés.

Cette première étape du tableau d'appréciation des risques est présentée à l'ensemble des interviewés. Cela permet d'échanger sur les pratiques des uns et des autres dans le laboratoire, toujours dans une volonté de sensibilisation et de démarche participative où les interviewés deviennent acteurs de la démarche. C'est un moment très riche de partage qui fait souvent émerger des discussions sur les solutions à adopter pour minimiser les risques observés sur certaines informations sensibles.

Au cours de cette réunion, les acteurs ont été formés au remplissage de ce tableau par la chargée de mission. Cette formation fait partie de la démarche. Les personnes interviewées peuvent alors valider les synthèses descriptives des activités décrites de leur métier, comme le veut la méthodologie ADAC. Ensuite, pour chaque information sensible, l'interviewé devra lui-même valoriser l'impact de cette information sur son métier et sur l'unité, en attribuant une valeur entre 0 et 4 pour le niveau de confidentialité, d'intégrité et de disponibilité de cette information sensible. L'interviewé devra ensuite valoriser, entre 0 et 2, la vraisemblance de la menace et la facilité d'exploitation des vulnérabilités associées déterminées par la chargée de mission.

Le canevas de ce tableau est issu d'une formation au management de la sécurité de l'information organisée par le CNRS et élaboré par François Morris, RSSI adjoint et Robert Longeon ex-chargé de mission SSI, tous deux au CNRS.

## 2.7 Résultats

Les tableaux d'appréciation des risques ont été élaborés par métier. Une moyenne des valeurs est réalisée entre les tableaux des interviewés d'un même métier. On obtient alors une cartographie par métier des informations sensibles à protéger, avec le niveau de risque associé entre 0 et 8 (8 correspond au niveau de risque maximum). En distribuant des niveaux de couleur aux niveaux de risques, ce tableau constitue un formidable outil de pilotage pour la gouvernance de l'unité de recherche.

Le tableau d'appréciation des risques global et anonyme est présenté lors d'une réunion d'étape à la direction de l'unité ainsi qu'au comité SSI et à l'ensemble des interviewés. Des échanges ont alors lieu sur l'élaboration d'un plan de traitements des risques.

A l'interne, les points de progrès et de réduction des risques concernent par exemple :

- sensibilisation des personnels ;
- sauvegarde des données automatiques des matériels de bureau et d'expérimentation + redondance ;

- politique d'archivage papier => classification – locaux dédiés avec contrôle d'accès ;
- mise en place d'une politique de chiffrement des matériels informatique « fixes », « portables », et des supports amovibles ;
- mise en place d'une politique d'archivage des cahiers de laboratoire et des échantillons ;
- sécurisation de l'usage de la visioconférence ;
- restructuration et/ou réaffectation des locaux ;
- gestion d'accès aux locaux (traces en entrée et en sortie de laboratoire) ;
- externalisation de la gestion de l'infrastructure réseau à la DSI de l'université ;
- mise en place d'une cogestion et d'un contrat de services ;
- externalisation de la messagerie et des services Web et mise en place d'un contrat de services ;
- gestion du courrier papier ;
- mise en place d'un serveur collaboratif pour la gestion des données à caractère personnel, des résultats de recherche, des contrats/brevets ;
- ajout d'un volet SSI dans tous les projets, contrat de service entre partenaires en plus de l'engagement de confidentialité.

La liste non exhaustive des points de progrès recensés constitue une véritable feuille de route pour la direction de l'unité de recherche.

## 2.8 Plan de traitement des risques

Le plan de traitement des risques permet à la gouvernance du laboratoire de recherche de choisir parmi les quatre traitements de risques possibles : acceptation, réduction, externalisation ou refus du risque.

Lors de l'acceptation du risque, le directeur d'unité décide de prendre le risque et en assume la responsabilité.

Dans le cas de la réduction du risque, le directeur décide de mettre les mesures techniques et/ou organisationnelles en place pour minimiser le risque et le rendre acceptable.

Le directeur décide d'externaliser le risque quand celui-ci n'est pas acceptable et que l'unité de recherche n'a pas les ressources ou les compétences en interne pour minimiser ce risque ou que cette activité n'est pas le cœur de métier du laboratoire de recherche. Le directeur choisit donc d'externaliser le risque soit vers la tutelle partenaire, soit dans une société privée. En se référant au guide de l'externalisation de l'ANSSI, le directeur sait qu'en choisissant l'externalisation, il ne désengage pas sa responsabilité. Il établira un contrat de service ou contrat d'externalisation avec son partenaire. Dans le cas où le directeur externalise vers la tutelle hôte, il a été décidé de mettre en place des contrats de service, au sens ITIL, afin de formaliser le partage des responsabilités entre tutelles, les clauses de sécurité de l'information et les conditions de services.

Lorsque la direction décide de refuser le risque, c'est qu'il souhaite arrêter un pan d'activité.

## 2.9 Elaboration de la Politique de Sécurité des Systèmes d'Information

En s'appuyant d'une part sur les mesures techniques et organisationnelles choisies par la direction de l'unité lors de cette démarche d'appréciation des risques, en associant les mesures techniques et organisationnelles définies par le CNRS dans sa PSSI d'établissement et en tenant compte des dispositions légales en matière de Sécurité de l'Information de l'ANSSI, la chargée de mission a pu élaborer un document de Politique de Sécurité des Systèmes d'Information de 8 pages pour chacune des unités. Cette PSSI se veut être un document pédagogique et évolutif.

Bien qu'elle reprenne les fondements de la PSSI de tutelle, la PSSI de l'unité de recherche représente le fruit d'un travail collaboratif et participatif au sein de l'unité. Elle reflète les spécificités propres du laboratoire de recherche dans son environnement, ses pratiques, son histoire. Dans toute conduite du changement, il est plus facile de faire adhérer des personnes qui se sentent acteurs de ce changement que subissant des directives loin de la réalité de terrain.

L'avantage d'une telle démarche restera avant tout le caractère pédagogique de sensibilisation de tous les acteurs du laboratoire et leur implication tout au long de la démarche y compris dans les choix de traitement. La richesse des résultats obtenus lors de cette étude sur un périmètre restreint de laboratoire, a contribué non seulement à assainir les pratiques métiers de l'unité, à définir une feuille de route des actions correctives et préventives à mettre en place dans un but d'amélioration continue, mais aussi à développer une culture de la sécurité de l'information et à faire prendre conscience de l'importance et de l'enjeu pour une université de mettre en place une Politique de Sécurité de l'Information d'établissement.

### **3 Vers la PSSI d'établissement**

Lors de sa mission PSSI dans des unités de recherche sensibles du CNRS, la RMSI a mis en évidence les flux d'informations sensibles entrant et sortant du périmètre de l'unité, notamment vers les services centraux de l'université, vers les tutelles, les collectivités territoriales, mais aussi vers les startups présentes à l'intérieur des laboratoires ou les pôles de compétitivités ou de valorisation de la recherche adossés aux unités ou à l'université.

Les informations sensibles, souvent des résultats de recherche extrêmement digérés donc brevetables, sortent du périmètre de l'unité ou de l'établissement vers le monde du privé. Les risques encourus par le potentiel scientifique et technique sont alors énormes.

La gouvernance de l'Université de Bourgogne a pris toute la mesure de ces enjeux en créant un Bureau de la Sécurité de l'Information et le poste de Responsable du Management de la Sécurité de l'Information.

#### **3.1 Elargissement du périmètre**

Afin d'avoir une cartographie précise des risques présents sur le périmètre de l'établissement, la Responsable du Management de la Sécurité de l'Information procèdera à une appréciation des risques de l'information sur diverses composantes de l'université. Les résultats de ces travaux contribueront à élaborer une Politique de Sécurité de l'Information de l'Université de Bourgogne sur la base des risques analysés et évalués sur son périmètre.

En prenant pour cadre la PSSI générique des établissements d'enseignement supérieur, la PSSI de notre établissement tiendra compte aussi de ses spécificités propres.

#### **3.2 Des chantiers en cours**

L'audit SSI réalisé par la RMSI a mis en lumière les dysfonctionnements liés à l'archivage papier. De nombreuses informations à caractère personnel sur support papier sont entreposées, non classifiées, gardées pour les besoins des audits financiers de tutelles et dupliquées sur l'ensemble de l'université dans chaque composante, sans être protégées dans des lieux sécurisés. L'Université de Bourgogne a recruté une archiviste qui travaille sur un guide d'archivage des données confidentielles dans le cadre de la sécurité de l'information ainsi que sur l'élimination des archives selon les règles de confidentialité. Un gros travail de dématérialisation doit par ailleurs être étudié au sein des tutelles.

De la même manière, l'archivage des cahiers de laboratoires, servant pourtant de preuve d'antériorité d'une découverte scientifique, n'est pas ou mal réalisé. Certains chercheurs vont même jusqu'à utiliser ou inventer des cahiers de laboratoires électroniques, jusqu'ici non reconnus juridiquement. Un travail de sensibilisation et d'archivage de ces cahiers et une étude sur la dématérialisation sont en cours.

Afin de réduire les risques et d'éviter les multiplications des clés, des badges, des passes et avoir une traçabilité des accès, l'Université de Bourgogne souhaite mettre en place une centralisation de la gestion des accès physiques aux bâtiments et aux bureaux. Pour cette raison, l'établissement s'est lancé dans le projet de déploiement d'une nouvelle carte multi services. Cette carte nominative sera utilisée comme système de contrôle d'accès physique aux bâtiments, mais aussi aux zones à régime restrictif présentes sur l'établissement jusqu'au bureau. L'infrastructure globale est actuellement à l'étude et répondra aux exigences de sécurité des technologies sans contact de l'ANSSI.

Un groupe projet travaille sur le chiffrement automatique des données transitant des ordinateurs fixes et portables vers les BYOD, les périphériques USB et les clouds.

## **3.3 Organisation de la Sécurité de l'Information à l'Université de Bourgogne**

### **3.3.1 Responsable du Management de la Sécurité de l'Information RMSI**

La mission principale de la RMSI est d'assurer la cohérence et le management de la sécurité de l'information matérielle et immatérielle de l'établissement. En relation avec tous les services concernés par la sécurité de l'information, la RMSI assure la mise en place d'une démarche qualité du Système d'Information de l'Université de Bourgogne répondant aux exigences du référentiel général de sécurité. Son positionnement est situé dans la gouvernance au niveau de la maîtrise d'ouvrage.

La RMSI assure la mise en place de la protection du potentiel scientifique et technique de l'établissement.

Elle définit la PSSI de l'établissement et pilote son déploiement sur l'ensemble du périmètre universitaire. Elle procède à l'analyse des risques et effectue des audits et contrôles en matière de sécurité de l'information.

Elle assure les rôles de conseil en sécurité, d'analyse de risques, d'étude de solution, de gestion des incidents de sécurité et de contrôle des conformités PSSI et CNIL, dans tous les projets relatifs aux systèmes d'information à l'interne et à l'externe vis-à-vis des prestataires et des partenaires.

Elle anime le réseau d'agents et d'équipes impacté par la sécurité du SI, assure la veille organisationnelle, juridique et technologique en matière de sécurité de l'information.

Enfin, la RMSI assure la sensibilisation des agents de l'établissement aux enjeux de la sécurité des systèmes d'informations, informe, conseille et alerte la gouvernance de l'Université de Bourgogne et les fonctions métiers sur les enjeux de la sécurité de l'information.

### **3.3.2 Le réseau des Chargés de Sécurité des Systèmes d'Information**

En dehors des acteurs opérationnels de la sécurité de l'information : CIL, AQSSI, FSD, la RMSI de l'Université de Bourgogne s'appuie non seulement sur les Responsables de Sécurité des Systèmes d'Information de l'établissement, mais aussi sur un réseau d'une quarantaine de CSSI (Chargés de Sécurité des Systèmes d'Information) nommés avec une lettre de mission dans les entités de l'université et dans les unités CNRS. Ce réseau assure une couverture complète du périmètre de l'établissement.

### **3.3.3 Le réseau des Gestionnaires Responsables de l'Information**

Par ailleurs, compte tenu du caractère transversal de sa mission et de l'impact de la sécurité de l'information sur l'ensemble des métiers présents à l'université, la RMSI met actuellement en place un réseau de GRI (Gestionnaires Responsables de l'Information). Ces personnes détiennent, de par leur métier, des informations sensibles et en sont responsables vis-à-vis de l'institution. Ils sont seuls à pouvoir définir en termes de confidentialité, d'intégrité et de disponibilité la valeur des actifs informationnels qu'ils manipulent au quotidien.

Ces deux réseaux de CSSI et de GRI constituent un relai essentiel dans la sensibilisation à la sécurité de l'information de tous les acteurs présents dans l'établissement. Une matrice de partage des responsabilités définit les périmètres d'actions de chacun de ces acteurs, ainsi que leurs rôles en termes de pilotage, de contribution ou de validation.

### **3.3.4 Les Comités de Sécurité de l'Information**

Un comité de pilotage stratégique a été créé permettant de développer un lieu d'échanges et de décisions concernant les choix liés aux risques majeurs sur la sécurité de l'information de l'établissement.

Des comités locaux ou comités SSI sont mis en place au fur et à mesure des avancées des analyses des risques sur le terrain. Ces comités sont animés par les CSSI nommés dans les entités et sont les vecteurs de la sensibilisation à la sécurité de l'information sur le terrain. Leur rôle est de gérer les incidents de sécurité au quotidien.

## **4 Conclusion**

L'Université de Bourgogne met en place une organisation de la sécurité de l'information capable de développer une culture de la sécurité de l'information au sein de l'établissement. Cette organisation et son management permettront non seulement de répondre à l'enjeu de Protection du Potentiel Scientifique et Technique, mais aussi d'asseoir une Politique de Sécurité des Systèmes d'Information connue et acceptée du plus grand nombre.

Les tutelles doivent réfléchir à l'urbanisation des Systèmes d'Information afin de répondre au mieux à l'évolution des métiers présents dans un établissement d'enseignement supérieur et de recherche et à la multiplication des collaborations publiques/privées dans un souci de sécurité de l'information en constante évolution.

## 5 Bibliographie

1. La norme ISO27001, ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements, <http://www.iso.org>
2. Management des risques, ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management, <http://www.iso.org>
3. ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls, <http://www.iso.org>
4. Analyse de l'activité et des compétences, Francis Minet, Education et Formation, Editions l'Harmattan, ISBN : 2-7384-3870-9
5. ITIL, pour un service informatique optimal, 2<sup>ème</sup> édition, Christian Dumont, Eyrolles
6. Guide ANSSI « Maitriser les risques de l'infogérance, Externalisation des systèmes d'information », décembre 2010, <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/>
7. Guide ANSSI « La sécurité des technologies sans contact pour le contrôle des accès physiques », novembre 2012, <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/>
8. Guide ANSSI « Guide d'hygiène informatique », janvier 2013, [http://www.ssi.gouv.fr/IMG/pdf/guide\\_hygiene\\_informatique\\_anssi.pdf](http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf)
9. Guide ANSSI « Recommandations de sécurité relatives aux ordiphones », juin 2013, [http://www.ssi.gouv.fr/IMG/pdf/NP\\_Ordiphones\\_NoteTech.pdf](http://www.ssi.gouv.fr/IMG/pdf/NP_Ordiphones_NoteTech.pdf)
10. CNRS, « Elaboration d'une PSSI opérationnelle d'unité », 23 mai 2008 Référence 08.2378/FSD, <https://aresu.dsi.cnrs.fr/IMG/pdf/Guide-elaboration-PSSI-operationnelle-unite.pdf>
11. CNRS, « Politique de Sécurité des Systèmes d'Information (PSSI-V1) », novembre 2006, [http://www.dgdr.cnrs.fr/FSD/securite-systemes/documentations\\_pdf/securite\\_systemes/PSSI-V1.pdf](http://www.dgdr.cnrs.fr/FSD/securite-systemes/documentations_pdf/securite_systemes/PSSI-V1.pdf)
12. CNRS, « Guide de l'intelligence économique pour la recherche », 2013, [http://www.cnrs.fr/derci/IMG/pdf/guide\\_intelligence\\_economique.pdf](http://www.cnrs.fr/derci/IMG/pdf/guide_intelligence_economique.pdf)