

Guide d'élaboration d'une PSSI opérationnelle d'unité

En date du 23 mai 2008

Référence 08.2378/FSD

Nature du document : Guide

Destinataires :

- Chargés de SSI dans les unités
- Coordinateurs Régionaux SSI

Mise en œuvre : Ce guide a pour objectif d'aider les acteurs de la SSI à élaborer une politique de sécurité des systèmes d'information qui soit opérationnelle dans leur unité.

Version 1.0

Sommaire

- I. – Préalables à l'élaboration d'une PSSI opérationnelle d'unité
 - 1. Compréhension des principaux concepts utilisés
 - 2. Liaisons entre PSSI d'organisme et PSSI opérationnelle d'unité
 - 3. Les 10 principes génériques d'une PSSI d'unité

- II. – Contenu d'une PSSI d'unité
 - 1. Organisation
 - 2. Périmètre de la PSSI
 - 3. Enjeux et menaces
 - 4. Sécurité physique
 - 5. Principes de mise en œuvre de la SSI
 - 6. Dispositions diverses

- III. En conclusion

ANNEXES

- A. – Plan type d'une PSSI d'unité
- B. – Exemple de PSSI opérationnelle
- C. – Gestion des risques en SSI : conseils de méthodologie

I - Préalables à l'élaboration d'une PSSI opérationnelle d'unité

1 – Compréhension des principaux concepts utilisés

→ L'appréciation des risques

L'appréciation des risques est l'approche méthodologique qui permet d'apprécier les menaces et leurs conséquences sur le système d'information de l'unité. Elle se conclue par une identification des objectifs et exigences de sécurité.

Diverses méthodologies sont utilisables dont celle s'appuyant sur la méthode EBIOS (élaborée par la Direction Centrale de la Sécurité des Systèmes d'Information du SGDN).

(**Remarque :** l'appréciation du risque est un travail *préalable* à la rédaction de la PSSI opérationnelle et doit faire l'objet d'un document séparé ; elle pourra s'inspirer des « conseil de méthodologie » proposés en annexe C).

→ Objectifs et exigences de sécurité

Les objectifs de sécurité expriment la volonté de couvrir les risques jugés inacceptables **sans préjuger des solutions pour y parvenir**. Ils découlent logiquement de l'appréciation des risques. Chaque risque inacceptable doit être associé à un objectif de sécurité visant à l'éliminer, le réduire ou le transférer à un tiers.

Exemples d'objectifs de sécurité :

1. le système ne peut tolérer une intrusion
2. le service de messagerie devra rester opérationnel.

Quant aux exigences de sécurité, elles sont exprimées de la manière suivante :

1. Le système est soumis à des tests d'intrusions utilisant les techniques connues
2. Le service de messagerie n'est pas indisponible plus de 24h.

→ Solutions de sécurité

Procédures, codes de conduite, règles de sécurité, normes, standards et dispositifs techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme. Elles sont construites par déclinaison des fonctions de sécurité dans un environnement et un contexte donnés. Elles n'ont pas à être détaillées dans une PSSI opérationnelle de façon à ne pas la surcharger.

→ PSSI opérationnelle

Une PSSI opérationnelle reprend, sans entrer dans les détails des procédures et dispositifs techniques, l'ensemble des fonctions ou des principes à mettre en œuvre pour satisfaire aux objectifs et exigences de sécurité. La PSSI opérationnelle est une déclinaison de la PSSI de l'organisme, en l'occurrence le CNRS.

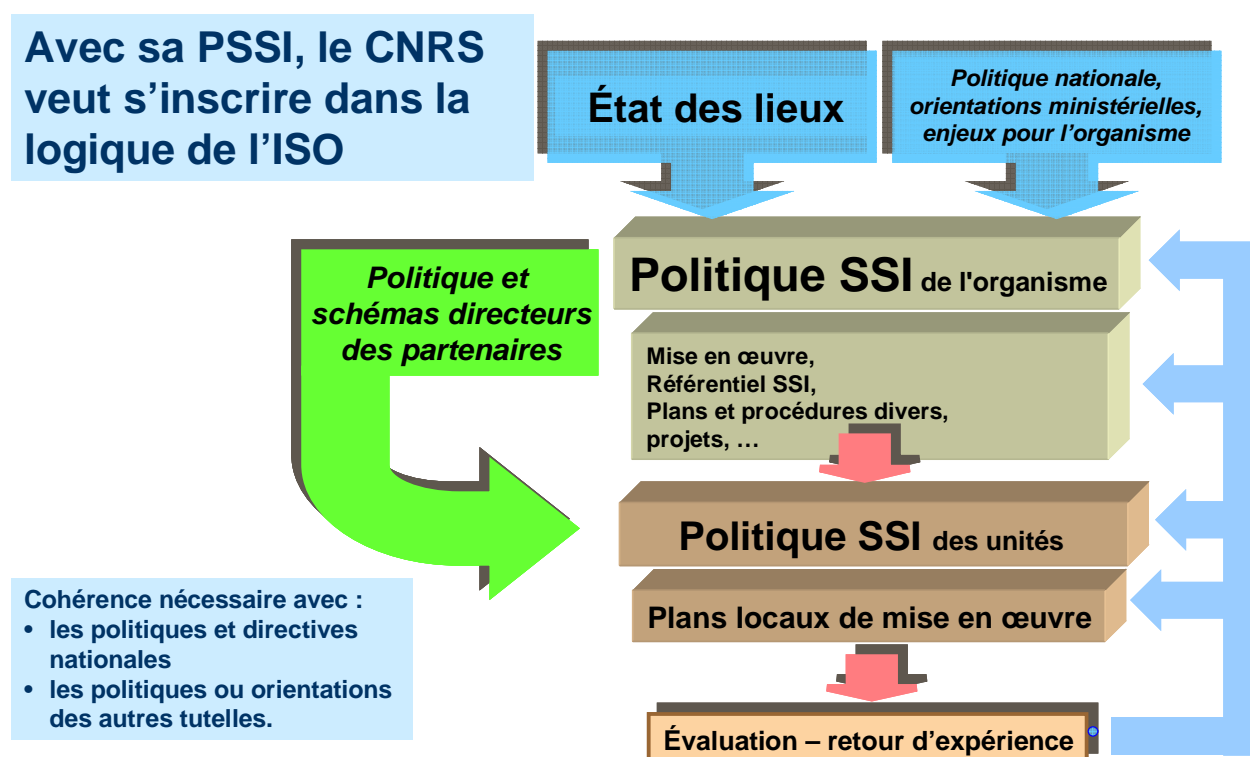
(Remarque : dans le cas d'Unités Mixtes de Recherche, la PSSI d'unité pourra le cas échéant se référer à un autre organisme de tutelle si cette tutelle a été reconnue « pilote » en matière de SSI. Ce cas est traité dans le chapitre « organisation » ci-après).

2 - Liaisons entre PSSI d'organisme et PSSI opérationnelle d'unité

La PSSI du CNRS le rappelle « La sécurité des systèmes d'information s'impose comme une composante essentielle de la protection du CNRS dans ses intérêts propres et dans ceux liés à des enjeux nationaux (intérêts fondamentaux de la nation) ». Elle relève d'une vision stratégique de l'organisme et traduit un engagement fort de la direction générale. Elle s'inscrit nécessairement sur le long terme.

Elle doit se décliner au niveau des unités, par une PSSI opérationnelle tenant compte des particularités propres à chaque unité et, pour ce qui est des unités mixtes, intégrant les orientations des autres tutelles. Le schéma suivant présente la déclinaison de la politique SSI d'un organisme dans les unités qui le compose. **Ce schéma s'applique aux unités propres du CNRS mais aussi aux unités mixtes relevant de la « tutelle SSI » du CNRS.**

Dans le cas d'une autre tutelle, le principe reste assez identique.



Au niveau de l'organisme la PSSI définit les objectifs stratégiques ou globaux et, en découlant, les « principes d'organisation et de mise en œuvre ».

Au niveau de l'unité, la PSSI traite de la mise en oeuvre **opérationnelle** de ces principes et de ces objectifs de sécurité (ou de ceux d'une autre tutelle de référence telles que les négociations au niveau régional en auront décidé). Elle a pour but de minimiser les risques de survenance d'un incident de sécurité ou, quand l'incident ne peut être évité, ses conséquences grâce à la préparation de plans de secours qui permettent de poursuivre malgré tout, les missions essentielles.

L'élaboration de la PSSI d'unité se fait donc à partir de la PSSI nationale en détaillant chaque rubrique en fonctions des objectifs de sécurité spécifique à l'unité ... en évitant de confondre « résultats à atteindre » et « moyens pour y parvenir ».

Il ne faut pas chercher à obtenir du premier coup une PSSI d'unité parfaite, elle doit s'affiner progressivement par des itérations successives du processus de conception.

3 –Les dix principes génériques d'une PSSI d'unité

Les dix principes qui suivent devraient vous permettre d'éviter les écueils classiques auxquels on se heurte quand on élabore une PSSI opérationnelle.

Principe n°1 : unicité du pilotage et de la politique de la SSI

Les négociations entre tutelles au niveau régional doivent permettre de définir, pour chaque unité mixte, quelle est la « tutelle de référence en SSI » ou, au minimum, quelle est la « matrice des responsabilités » liées aux différentes tâches de pilotage de la SSI, de façon à respecter le principe « d'unicité des responsabilités », principe sans lequel aucun pilotage n'est possible.

Ce principe d'unicité ne signifie pas pour les autres tutelles un abandon de leurs droits à l'information (notamment sur les incidents de sécurité dont a été victime l'unité).

Des unités peuvent rencontrer des difficultés d'identification de ce pilotage, lorsque les négociations n'ont pas encore abouti. Cela n'interdit pas le « lancement » du travail de constitution de la PSSI au niveau local en particulier l'identification des enjeux propres à l'unité, l'appréciation des risques et l'ébauche des objectifs de sécurité. En revanche, la PSSI devant intégrer les principes de la PSSI de tutelle et faire référence à cette tutelle, dans une situation transitoire où l'unité est orpheline, il ne peut y avoir de PSSI locale validée.

Dans une telle situation, la direction de l'unité, en liaison avec la délégation régionale, peut négocier avec les autres tutelles une PSSI locale liée au CNRS, par défaut.

Principe n°2 : une PSSI opérationnelle énonce ce qu'il faut obtenir, non comment l'obtenir

Le rôle d'une PSSI opérationnelle est d'énoncer les résultats de sécurité attendus, non les moyens pour les obtenir. Il faut donc distinguer la *politique* qui décrit les fonctions et les principes qu'il faut mettre en œuvre pour réaliser les objectifs de sécurité, des *solutions de sécurité*.

Par exemple on exprimera une fonction de sécurité de la manière suivante : « *l'accès à distance au réseau interne est autorisé à la condition impérative d'une authentification forte des utilisateurs et d'une connexion réseau chiffrée* » **mais on ne dira pas** « *l'accès externe au réseau est authentifié par un certificat délivré par l'IGC du CNRS et se fait par une liaison VPN* »

Le fait que la PSSI opérationnelle exprime des principes – par nature durables – indépendamment des solutions de sécurité – qui, elles, suivent les évolutions des architectures, des technologies ou des savoir-faire - assurent à la PSSI une plus grande pérennité et une meilleure lisibilité. Ce point est important car il ne faut pas oublier que le public auquel elle s'adresse (utilisateurs du SI et la direction de l'unité) n'est pas, a priori, spécialiste de la question.

Principe n°3 : la réalisation d'une PSSI est un acte de direction

La PSSI d'unité doit être approuvée par le Directeur d'une manière officielle (approbation confirmée par le conseil de l'unité). De plus il s'engage à veiller à son respect.

Principe n°4 : la charte utilisateur est partie intégrante de la PSSI

La Charte utilisateur qui énonce la « loi commune » régissant l'utilisation des moyens informatiques, est le prolongement réglementaire et juridique de la PSSI d'unité.

Principe n°5 : une PSSI est contrôlable

Les objectifs de sécurité doivent être clairs, précis et justifiables, de manière que la mise en œuvre soit contrôlable et qu'une « métrique », essentiellement des indicateurs associés aux objectifs de sécurité (appelés « tableau de bord ») puissent permettre de juger du niveau réel de la SSI.

A cette condition, il est possible de « piloter » la sécurité.

L'application de la PSSI locale est susceptible d'audits par les représentants de la chaîne fonctionnelle SSI du CNRS ou encore par la cellule d'audit du CNRS.

Principe n°6 : la PSSI est réaliste

Si les recommandations nationales s'imposent, les objectifs assignés localement doivent rester cohérents avec les moyens disponibles et résulter d'un arbitrage entre les moyens mis en œuvre et les gains de sécurité attendus. Il convient d'éviter d'afficher des consignes théoriques manifestement démesurées.

Principe n°7 : la PSSI est évolutive

La PSSI est évolutive et doit être révisée en fonction des enseignements tirés de l'expérience passée, de l'évolution de l'environnement et du contexte (évolution des menaces, évolution de la réglementation, de la jurisprudence) et de l'actualisation des directives nationales.

Principe n°8 : savoir gérer les exceptions !

Quelle que soit la PSSI adoptée, il faut savoir gérer les exceptions ou dérogations aux principes de sécurité. Toutefois, ces exceptions ne doivent pas devenir la règle ; elles font l'objet d'un référencement et doivent être contrôlées, en liaison avec la chaîne fonctionnelle SSI.

Principe n°9 : la PSSI d'unité est un document pédagogique

- Une PSSI qui, tant par son vocabulaire abscons que par son formalisme, tient plus de « la gnose » que de la SSI,
- Une PSSI qui n'est connue que « des initiés et de leur gourou »,
- Une PSSI qui semble n'avoir aucune prise sur le réel,

Une telle PSSI n'a aucune chance d'être appliquée dans l'unité. Pire, elle risque de devenir un repoussoir de la sécurité pour les « non-initiés ».

Une PSSI opérationnelle est aux antipodes de cette approche. Ce doit être un document de communication et de sensibilisation qui a vocation à être connu et partagé par tous ceux qui, d'une manière ou d'une autre, en tant qu'utilisateurs ou en tant que décideur, interviennent sur le système d'information. Elle doit donc être assez courte (une quinzaine de pages maximum), claire, synthétique et pédagogique.

Principe n°10 : la PSSI d'unité doit être une œuvre collective

L'élaboration de la PSSI n'est pas une entreprise solitaire ou un exercice de style mais une démarche qui doit engager l'ensemble de l'unité, y compris (et surtout) les responsables.

A l'inverse, une équipe projet trop nombreuse génère des réunions lourdes et inefficaces et une bureaucratie stérilisante.

Il faudra donc trouver un juste compromis entre le nombre et la solitude ... sans oublier que l'essentiel reste dans le mode opératoire :

1. Le « projet PSSI » doit être « léger », générer un minimum de bureaucratie et de paperasserie, et surtout ne pas traîner en longueur (une durée de deux mois devrait être suffisante).
2. Dans une unité de recherche, le projet doit être décidé en réunion de laboratoire (le mieux serait en conseil de laboratoire) avec une forte implication de la direction. Durant cette réunion, le directeur de l'unité annonce par exemple officiellement la nomination du CSSI (en insistant sur la nouvelle dimension que lui confère l'organisation fonctionnelle de la SSI au CNRS telle qu'elle est décrite dans la PSSI de l'organisme) et présente le projet dans ses différentes phases.
3. Une équipe de projet de quelques personnes représentatives (moins de 6) animée par le CSSI, qui conduira le travail d'élaboration du document PSSI, est constituée. Elle validera le travail : étude de l'existant, appréciation des risques, PSSI ainsi que les différents éléments du référentiel SSI de l'unité.
4. Des réunions avec les utilisateurs comportant une forte implication de la direction devront ponctuer chaque étape importante du projet (en particulier lors de la validation du travail effectué).

II - Contenu d'une PSSI d'unité

1 – Organisation

1.1 - Organisation interne

Pour commencer, il faut rappeler que le directeur est le responsable de la SSI de son unité et dire que pour assumer cette responsabilité, il s'appuie sur le Chargé de SSI (CSSI) de l'unité.

On aura en tête le principe d'unicité qui conduit à avoir un seul CSSI représentant l'unité vis-à-vis de toutes les tutelles..

On détaillera l'organisation interne de la SSI et les relations entre acteurs, par exemple dans le cas d'unités disposant de plusieurs implantations (résultant de fusions de laboratoire par exemple) il peut être utile de désigner des correspondants du CSSI dans certaines implantations. Il peut aussi être utile, selon la taille de l'unité, de désigner un ou plusieurs suppléants. Les rôles de chacun doivent être précisés, de même que les liens avec les administrateurs systèmes et réseaux.

Pour ce qui est du rôle du CSSI on reprendra (avec adaptations locales si nécessaires) le rôle tel que décrit dans la PSSI du CNRS.

Si le CSSI dispose d'une « lettre de mission » de son directeur, cette lettre peut être reprise ou annexée à la PSSI de l'unité.

Si des habilitations de défense sont nécessaires, il conviendra de le signaler (« le poste exige une habilitation « confidentiel défense » »)

Dans le cas d'unités de faible taille et selon la disposition des structures locales (partage d'un même bâtiment et d'un même réseau avec d'autres unités) on peut exceptionnellement « mutualiser » la fonction de CSSI. Cette mutualisation doit alors être décrite. Il est possible d'ailleurs de réaliser un document de PSSI mutualisé. En revanche chaque directeur reste responsable de la SSI de son unité, il restera signataire de la PSSI de son unité et validera le fait que son unité intègre un périmètre plus large.

1.2 - Place de la PSSI d'unité dans la chaîne fonctionnelle SSI

L'unité de recherche s'inscrit dans une organisation, la PSSI de l'unité s'inscrit dans une politique nationale définie par le Secrétariat Général de la Défense Nationale (SGDN) et le Haut Fonctionnaire de Défense et de Sécurité (HFDS) du ministère chargé de la recherche, et dans la politique de la ou des tutelles de l'unité.

Il convient en tout premier lieu d'afficher ce lien avec la politique et les directives nationales en explicitant pour l'unité **la tutelle de référence en matière de SSI**.

En affichant cette tutelle, l'unité situe sa propre politique dans celle de sa tutelle, et se rattache à la chaîne fonctionnelle SSI de cette tutelle.

Ce rattachement doit être cité et explicité. S'il s'agit du CNRS il faudra rappeler le lien avec la coordination régionale et le CMSSI/FSD.

S'il y a partage de responsabilité entre tutelles, il conviendra de décrire ce que recouvre ce partage (via une « matrice de responsabilités » par exemple, qui sera annexée à la PSSI)

Ce point est essentiel car le directeur de l'unité ne peut signer une PSSI isolée de tout contexte et de toute tutelle. En revanche il est possible de lancer la constitution d'une PSSI opérationnelle d'unité sans attendre l'issue de négociations entre tutelles pour définir la tutelle PSSI.

La désignation d'une tutelle pilote n'implique pas le désintérêt des autres tutelles vis-à-vis de la SSI de l'unité.

On décrira donc, pour les unités mixtes, les dispositions de coordination avec les autres tutelles prévues et en particulier la circulation de l'information (les tutelles non pilotes sont au minimum destinataire de la PSSI d'unité et tenues informées des incidents importants, des dépôts de plainte etc...)

2 - Périmètre de la PSSI

Nos systèmes d'information sont très fortement imbriqués, à l'intérieur même des unités du fait des rattachements à des tutelles différentes et, à l'extérieur, par les connexions aux réseaux de nos divers partenaires et aux nombreux réseaux d'accès.

Une PSSI doit décrire d'une manière claire, nette et précise ce qui est à protéger, c'est-à-dire, ce sur quoi a porté l'appréciation des risques d'où ont découlé les objectifs de sécurité. C'est ce qu'on appelle « le périmètre de sécurité », frontière qui sépare « l'intérieur » de « l'extérieur » du SI.

Ce périmètre doit rester cohérent avec le périmètre général défini dans la PSSI du CNRS (chapitre I.2)

Certains éléments du Système d'Information de partenaires industriels ou de recherche peuvent être intégrés au périmètre de sécurité pour des raisons de souplesse des procédures, mais dans ce cas ces matériels, ces applications ou ces données devront avoir les mêmes contraintes de sécurité que le réseau interne.

On entre dans le périmètre de sécurité et on en sort par « un sas » dont la sécurité est évidemment renforcée et correctement surveillée.

3 – Enjeux et menaces

La PSSI d'unité doit rappeler ici de manière succincte les enjeux de la sécurité des systèmes d'information pour l'unité, au regard des menaces spécifiques qui peuvent peser sur elle et en tenant compte des spécificités et valeurs du patrimoine scientifique de l'unité.

Pour des raisons de confidentialité, il ne sera pas fait référence – de manière explicite – au classement de sensibilité du laboratoire, mais on pourra parler de « laboratoire particulièrement sensible au regard du patrimoine scientifique » lorsque le laboratoire est ERR, de « laboratoire sensible » si le laboratoire est ES et de « laboratoire non classé sensible » s'il s'agit d'un ERO.

Pour les laboratoires sensibles et particulièrement sensibles, les justifications de sensibilité pourront être évoquées là encore de manière succincte, en évitant de citer des informations qui pourraient être de nature confidentielle.

Ce travail d'identification des enjeux et menaces constitue la première étape de la gestion des risques (cf. annexe C : « gestion des risques : conseils de méthodologie »).

L'important à ce stade est de présenter les enjeux et priorités de protection pour l'unité en décomposant par exemple ce qui peut concerner :

- les informations
- les fonctions
- les systèmes
- les infrastructures de l'unité

A titre d'exemples, en matière « d'informations », si l'on traite d'informations très sensibles de type « défense », ou relevant de la propriété intellectuelle, quelle valeur est attachée à la possession de ces données, à leur intégrité, à leur non-divulgaration, on pourra de même mettre l'accent sur des infrastructures d'importance majeure qui pourraient être rendues indisponibles par un incident informatique...

Ce travail initial exploratoire devra toutefois être repris une fois l'appréciation des risques achevée pour corriger ou compléter cette évaluation, en incorporant par exemple de manière très synthétique les résultats de l'analyse de risque.

Le document de PSSI opérationnelle a vocation à être largement diffusé dans l'unité, ce paragraphe est donc important car il introduit et justifie les principes de mise en œuvre définis ensuite dans le document de PSSI.

4 - Sécurité physique

On entend par « Sécurité physique » l'ensemble des moyens pris ou à prendre sur les installations pour éviter la survenance d'une malveillance, d'un accident ou d'un sinistre ayant des conséquences sur les installations techniques nécessaires au fonctionnement du système d'information (locaux, machines de traitement de l'information, supports informatiques, réseaux, périphériques, équipements logistiques et de communication, etc.) ou à défaut, pour intervenir le plus efficacement possible dès sa survenance.

Il peut être utile de mettre en place des périmètres de sécurité physique à accès restreints éventuellement équipé de caméras¹.

Les ressources critiques (serveurs, équipements télécoms, etc.) doivent être placées dans des locaux à accès contrôlés.

Toute modification physique d'infrastructure doit être identifiée, validée et consignée.

Le plan de sécurité physique (qui doit être élaboré en concertation avec l'ingénieur « prévention et sécurité »), quand il en existe un, fait partie du « référentiel sécurité » de l'unité. La PSSI doit alors le mentionner mais il n'est pas souhaitable de l'intégrer « in extenso » à la PSSI de façon à ne pas l'alourdir.

5 – Principes de mise en œuvre de la SSI

On rappellera que les dispositions définies au chapitre II.4 de la PSSI du CNRS sont d'application effective dans l'unité. Si certaines dispositions diffèrent, il convient de le citer et d'explicitier les dispositions propres à l'unité et le cas échéant en dérogation avec les directives nationales. En cas de dérogation, il conviendra de soumettre les propositions de rédaction à la chaîne fonctionnelle SSI (au moins au niveau de la coordination régionale).

Le plus simple est de reprendre les dispositions nationales, en les adaptant et en les explicitant et en les complétant si nécessaire au niveau local. En revanche il n'y a pas lieu de reprendre les dispositions nationales d'ordre général qui ne concernent pas l'unité.

¹ Les fichiers liés à la vidéosurveillance doivent être déclarés à la CNIL. Leurs traitements doivent être « proportionnés » aux objectifs poursuivis. Il faut rappeler régulièrement que la SSI, n'est pas la cybersurveillance des salariés ... et que tout détournement de finalité est un délit grave.

Pour ce qui est de la sécurité des données et des réseaux, on décrira ici l'ensemble des « *fonctions et des principes* » déclinant des objectifs et exigences de sécurité tels que de la PSSI générale les a identifiés ou ceux, plus spécifiques, qui ont nécessité une analyse de risque particulière.

La place de la charte utilisateurs et les dispositions de mise en œuvre (annexe au règlement intérieur par exemple) pourront faire l'objet d'un développement spécifique.

Par ailleurs le chapitre II.4.4 de la PSSI nationale (« Mesure du niveau effectif de sécurité ») pourra trouver sa place de déclinaison dans l'unité dans une partie finale du document de PSSI d'unité (« Dispositions diverses »)

On pourra s'inspirer du plan type proposé en annexe A du présent document.

6 - Disposition diverses

Si la partie II.4.4 de la PSSI nationale n'a pas été intégrée plus haut, il peut être utile de terminer le document de PSSI opérationnelle par les aspects relatifs aux dispositions de contrôle et à celles liées à la posture de sécurité et gestion de crise, et en intégrant le cas échéant à ce niveau des dispositions générales de type gestion de crise, gestion de la documentation.

Sur la question des tableaux de bord², il faut arriver à construire un système d'indicateurs qui permettent de vérifier les points clés de la PSSI. Pour cela on utilisera utilement les traces des tests de vulnérabilité et du système de détection d'intrusion qu'on organisera de façon à mettre en évidence le nombre de vulnérabilités détectées, le pourcentage des équipements touchés, le nombre moyen de vulnérabilités par équipement, le nombre total de vulnérabilités détectées par niveau d'impact, etc.

Les traces récupérées sur les équipements d'extrémité de réseau pourront permettre d'évaluer le nombre d'attaques détectées par équipement ou par type d'équipement, le nombre d'attaques par service réseau, le nombre de commandes critiques par équipement et par utilisateur, etc.

D'autres indicateurs peuvent encore être utilisés comme aide au pilotage de la sécurité :

- nombre de sensibilisations, de formations, d'actions d'information, etc.
- évolution du nombre de personnes formées,
- indicateurs RENATER : alertes RENATER non détectées en interne,
- indicateurs de temps de résolution d'un incident de sécurité, du délai de prise, en compte de l'incident, etc.

² Le rôle des tableaux de bord est de mesurer l'état de la SSI pendant une période donnée à partir de critères de nature différente. Un ensemble d'indicateurs ne peut appréhender la complexité de la SSI sans perte d'information. De ce point de vue un tableau de bord est forcément réducteur aussi doit-on garder un recul prudent dans l'interprétation des résultats :

- faire la différence entre mesures (qui peut être qualitatif) et métrique (qui est quantitatif)
- se méfier des valeurs moyennes (par exemple : moyenne entre un risque élevé et un risque faible !)
- prendre les systèmes automatiques (SIM, IDS, etc.) pour ce qu'ils sont : des outils d'aide au pilotage de la sécurité non des substituts à la réflexion.

On choisira les indicateurs en fonction des éléments particuliers de la sécurité qu'on veut apprécier :

- mesurer l'évolution de la situation (menaces, niveaux de sécurité, impact, ...),
- surveiller les éléments critiques,
- mesurer les écarts entre des objectifs et une situation donnée,
- constituer des systèmes d'alerte pour organiser « une défense en profondeur ».

III - En conclusion

Implémentation des solutions de sécurité – plans d’actions SSI -

Il restera à implémenter les mesures concrètes (règles, procédures, dispositifs techniques) qui permettent de réaliser ces fonctions de sécurité. Ceci doit être fait sous les contraintes – en principe prises en compte dans la phase de l’appréciation des risques - des moyens (humains, techniques et budgétaires), de l’organisation du CNRS et de sa politique en matière de SSI, des politiques des divers partenaires, du temps et des compétences disponibles, de la réglementation, etc.

La PSSI est un cadrage et un point de départ, au-delà il y a l’implémentation des solutions de sécurité - véritable « projet SSI d’unité » - avec l’accompagnement d’un tableau de bord et le nécessaire retour d’expérience. Ces mesures de mise en œuvre (qui ne font donc pas partie de la PSSI d’unité) peuvent utilement être intégrées dans le cadre d’un plan d’actions interne SSI planifiant les actions à mener, les objectifs visés, les moyens à mettre en œuvre et le mode de mesure de l’atteinte des objectifs.

Rappelons que :

- La sécurité c’est :
 - 20% de technique et 80% de bon sens et d’organisation ;
 - une affaire qui relève de la direction : il n’est pas possible d’assurer la sécurité dans les unités où celle-ci ne se sent pas concernée ;
 - une question d’état d’esprit collectif : dans 99% des cas un incident de sécurité a pour origine une erreur ou une négligence humaine.
- Et que :
 - la sécurité à 100% n’existe pas, le risque 0 non plus ;
 - gérer la sécurité est l’art de gérer le risque ;
 - il n’y a nécessairement un compromis entre la valeur de l’information ou du système protégé et le coût de la protection ;
 - il y a rien de plus dangereux que de répondre à de mauvais besoins par de mauvaises solutions ;
 - la sécurité d’un système est une chaîne.

Annexe A

Exemple de plan d'une PSSI d'unité

1) Organisation

- 1.1 - Organisation interne
- 1.2 - Place de la PSSI d'unité dans la chaîne fonctionnelle SSI

2) Périmètre de la SSI dans l'unité X

3) Enjeux et menaces

4) Sécurité physique

5) Principes de mise en œuvre de la SSI

- 5.1 Principes organisationnels
 - 5.1.1 - Conditions d'accès
 - 5.1.2 - Charte informatique
- 5.2 Politique de sécurité des données
 - 5.2.1 - Protection des données sensibles
 - 5.2.2 - Protection des données à caractère personnel
 - 5.2.3 - Politique de sécurité des postes de travail
 - 5.2.4 - Politique de sécurité des supports amovibles et des matériels nomades
 - 5.2.5 - Politique de sécurité des serveurs
 - 5.2.6 - Politique de sécurité des applications
 - 5.2.7 - Politique de sauvegarde, d'archivage et de restauration
 - 5.2.8 - Réparation, cession, mise au rebut des matériels de stockage³
- 5.3 - Politiques de sécurité réseau
 - 5.3.1 - Politique de gestion du trafic sur les réseaux internes
 - 5.3.2 - Politique d'accès à distance aux réseaux internes
 - 5.3.3 - Politique de sécurité des réseaux sans fil :
 - 5.3.4 - Politique d'accès à Internet depuis le réseau interne
 - 5.3.5 - Sécurité des infrastructures réseaux et télécoms

6) Dispositions diverses

- 6.1 - Procédure de traitement des incidents et plans de gestion de crise
 - 6.1.1 - Gestion d'incidents
 - 6.1.2 - Gestion de crise
 - 6.1.3 - Plan de continuité
- 6.2 - Maintient du niveau de sécurité
 - 6.2.1 - Sensibilisation et formation des utilisateurs

³ Il est fait ici référence aux matériels de stockage, mais d'autres matériels comme les routeurs peuvent aussi être concernés : les « access list » ne sont forcément à mettre sur la place publique.

- 6.2.2 - Posture de sécurité
 - 6.2.3 - Mises en garde et recommandations de la chaîne fonctionnelle
- 6.3 - Mesures du niveau effectif de sécurité
 - 6.3.1 - Contrôle de gestion de la SSI
 - 6.3.2 - Audits
 - 6.3.3 - Journalisation
 - 6.3.4 - Tableaux de bord
- 6.4 Maintenance et développement
 - 6.4.1 - Téléactions internes
 - 6.4.2- Infogérance et télémaintenance externes
 - 6.4.3- Développement d'applications
 - 6.4.4- Clauses dans les marchés
- 6.5 Référentiel SSI et gestion de la documentation SI

Annexe B

Exemple de PSSI opérationnelle

Le présent document constitue la PSSI du laboratoire ERROR (**E**tude et **R**echerche en **R**éaménagement et **O**rganisation **R**urale), UMR007, unité mixte de recherche sous tutelle du CNRS, de l'Université de Montcanin et de l'ENSMC (Ecole Nationale Supérieure de MontCanin).

Cette PSSI opérationnelle est prise en application de la politique de sécurité des systèmes d'information du CNRS.

Elle est évolutive et susceptible de mises à jour en fonction des évolutions d'ordre interne ou externe touchant la PSSI (en particulier évolutions de l'activité du laboratoire, évolution des directives et plans nationaux).

Les écarts entre les objectifs de sécurité tels que le propose la PSSI et le niveau réel de sécurité sont estimés au moyen d'un ensemble d'indicateurs appelé tableau de bord, mis en place conjointement à la PSSI.

1. - Organisation et responsabilités des différents acteurs

1.1 - Organisation interne

Le directeur est le responsable de la SSI de l'unité.

Pour assumer cette responsabilité, il s'appuie sur le Chargé de SSI (CSSI).

Au titre de CSSI, ses missions sont les suivantes :

- promouvoir la mise en place de la PSSI d'unité,
- veiller à ce que les mesures de sécurité nécessaires soient correctement mises en place,
- veiller à l'application des instructions et recommandations,
- veiller à la bonne exploitation des avis des CERT RENATER et CERTA,
- sensibiliser les utilisateurs,
- s'assurer des réactions adéquates lors du traitement des incidents et en cas de déclenchement du plan de crise,
- veiller à la prise en compte de la sécurité dans la rédaction des contrats de sous-traitance et les cahiers des charges des applications,
- veiller au respect des formalités requises par la loi Informatique et Libertés pour les traitements de données à caractère personnel,
- assurer la veille en matière de SSI et les niveaux relationnels nécessaires en liaison avec la coordination générale et plus généralement la chaîne fonctionnelle SSI.

Compte tenu de la structuration du laboratoire en deux implantations géographiques, le CSSI dispose d'un relais à l'antenne de l'ENSMC. Celui-ci supplée le CSSI en son absence.

Un comité d'orientation de la SSI, présidé par l'Adjoint au directeur et dont le CSSI assure le pilotage, est l'instance collective de suivi de la SSI pour le laboratoire. Le projet de PSSI ainsi que les projets de

modificatifs sont soumis à ce comité, de même que le programme annuel de SSI. Le comité approuve également le rapport annuel de la SSI de l'unité.

1.2 - Place de la PSSI d'unité dans la chaîne fonctionnelle SSI

Le CNRS a été désigné comme « tutelle de référence SSI » de l'UMR007 en application des accords cadres conclus entre la délégation régionale du CNRS et l'université de Montdenis. L'université de Montdenis garde son droit de contrôle et d'approbation du pilotage effectif de la SSI et devra être informée de tous les incidents significatifs dont sera victime l'unité.

L'antenne à l'ENSMC reste sous la tutelle SSI de l'école.

Le CSSI de l'unité intègre la chaîne fonctionnelle SSI du CNRS qui est structurée au niveau régional par le coordinateur régional SSI sous la direction du délégué régional et au niveau national par le chargé de mission SSI sous la direction du FSD du CNRS.

Les acteurs intervenant en matière de sécurité des systèmes d'information, au titre d'autorité hiérarchique ou au titre de la chaîne fonctionnelle sont liés à leur devoir de réserve voire à des obligations de secret professionnel. Ils peuvent si nécessaire faire l'objet d'une habilitation au secret de défense.

2. - Périmètre de la SSI dans l'unité ERROR

Le périmètre de la SSI de l'UMR007 exclut les services réseaux fournis par l'université tels que :

- Les réseaux de télécommunications (y compris la téléphonie) ne sont pas gérés par l'unité ;
- Connectivité aux principaux réseaux : de campus, métropolitains, nationaux et internationaux ;
- Les serveurs de l'ensemble des tutelles et de ses partenaires mis à disposition de l'unité pour assurer sa gestion administrative, financière, de ses congrès ou de ses publications ;
- Serveurs hébergés par l'unité mais administrés par la structure de valorisation « ERRARE ».

En revanche, font partie du système d'information de l'unité, l'enregistrement des traces et de ses travaux de recherche ainsi que de toutes les ressources gérées en interne tel que :

- Espace de travail (équipements, logiciels et supports),
- Espace de stockage et d'archivage (équipements, logiciels et supports),
- Serveurs (équipements et logiciels) web, messagerie électronique et autres services de communication lorsque les serveurs sont sous la responsabilité de l'unité,
- La base de données de gestion des abonnés à la revue Error-Research éditée par l'unité,
- Les applications et systèmes tournant sur les matériels gérés par l'unité,
- Le système de pilotage (contrôle commande) du banc de test du laboratoire,
- Les données personnelles, qu'elles soient dans des bases de données ou dans des fichiers informatiques.

Les ordinateurs portables des visiteurs, des congressistes et de tout autre invité du laboratoire sont exclus du périmètre de sécurité. L'accès à Internet leur est offert par une connexion au réseau d'accueil, isolé du système d'information. En revanche, lorsqu'un utilisateur est amené à connecter son ordinateur portable, même personnel, à un réseau permettant d'accéder aux informations de l'unité, ce matériel fait partie du système d'information de l'unité et de ce fait est soumis à la présente politique de sécurité.

Les systèmes d'information des collaborations de recherche ne font pas partie du périmètre de la SSI.

3. – Enjeux et menaces

Le laboratoire d'Etude et Recherche en Réaménagement et Organisation Rurale est un laboratoire particulièrement sensible, notamment du fait d'applications duales⁴ possibles de ses travaux et de contrats industriels avec des partenaires du secteur défense.

Certaines recherches du laboratoire, en particulier celles du département « villes à la campagne », concernent des technologies particulièrement innovantes (les recherches en cours sur « l'enfouissement total des logements collectifs dans des collines artificielles constituent une avancée majeure en matière d'urbanisme rural) et le laboratoire dépose régulièrement des brevets. Le laboratoire dispose d'ailleurs d'une équipe de valorisation en contact avec le Service des Partenariats et de la Valorisation de la délégation et la cellule de valorisation de l'ENSMC.

Le laboratoire conduit des coopérations internationales dont certaines avec des pays « sensibles », de nombreuses missions de chercheurs se situent dans ce cadre et le laboratoire accueille chaque année une soixantaine de stagiaires étrangers, dont une trentaine de thésards.

Le laboratoire ERROR met en ligne une base de données de dimension internationale dont les données sans être confidentielles ont une forte exigence de disponibilité et d'intégrité.

Le laboratoire ERROR abrite, dans son antenne à l'ENSMC une plateforme d'essais qui a une vocation régionale et dont la disponibilité permanente doit être préservée.

Les enjeux essentiels de la SSI pour le laboratoire résident :

- dans la protection des données scientifiques et industrielles sensibles (tant en matière de technologies à caractère dual que vis-à-vis des informations préalables à des dépôts de brevets) Ceci concerne plus particulièrement les départements « béton à décomposition rapide » et « ville à la campagne », le département « huttes et nouvel habitat » conduisant des recherches de nature plutôt fondamentale, sans caractère de sensibilité. Les menaces majeures identifiées peuvent être d'origine externe (compromission ou vols de données) mais aussi internes (présence de nombreux personnels non permanents...).
- dans la protection des fonctions et outils informatiques du laboratoire, en particulier le réseau informatique du laboratoire, la base de données internationales et le fonctionnement de la plateforme d'essai.
- dans la protection des données relevant des ressources humaine (administration, gestion, santé, etc.).

La nature très ouverte du laboratoire (site universitaire ou école) et la présence de nombreux stagiaires sont des facteurs de vulnérabilité.

4. - Sécurité physique

Le CSSI conçoit, formalise, organise et contrôle en concertation avec l'ingénieur « prévention et sécurité » les plans de sécurité physique de toutes les installations techniques situées dans son champ d'action afin d'éviter :

- un dommage causé par l'action de l'homme (erreur humaine, vandalisme, sabotage, chute d'objet, etc.),
- les risques de vol sous toutes les formes,
- un arrêt ou un dommage pour cause d'interruption d'électricité,
- une surchauffe par la mise en place d'une climatisation adaptée⁵.

⁴ Une application est dite duale lorsqu'elle peut être à double usage, l'un civil et l'autre militaire.

⁵ Ici on pense à une panne pendant le week-end de la climatisation dans la salle des serveurs qui entraînerait une surchauffe très préjudiciable aux matériels.

Le plan de sécurité physique comprend également les procédures d'intervention en cas de perturbation grave, en particulier les procédures pour avertir les personnes compétentes (personnel interne, chaîne hiérarchique, chaîne fonctionnelle, etc.)

5. – Principes de mise en œuvre de la SSI

5.1 - Principes d'organisation

5.1.1 - Conditions d'accès

Toute personne, qu'elle soit personnel permanent ou non, CNRS ou non, devant travailler sur des équipements connectés au réseau informatique de l'unité peut disposer d'un compte utilisateur, sous réserves d'avoir signé la charte informatique du CNRS, actant ainsi sa prise de connaissance de ses droits et devoirs d'utilisateur.

La condition générale d'accès au système d'information de l'unité est déterminée par un profil utilisateur. Un profil ouvre des droits d'utilisation de moyens technique, de consultation ou/et de modification de données et d'utilisation de services divers dont les services réseau. Les profils sont gérés pour tenir compte des évolutions de situation (en particulier du départ ou des changements de fonction de l'utilisateur)⁶.

L'accès à un profil se fait par identification/authentification. L'authentification est assez sûre pour ne pas être « cassée » par force brute avec des moyens ordinaires. Une procédure minimise les conséquences de la perte (ou du vol par écoute passive du réseau) d'un couple Identifiant/authentifiant et les utilisateurs sont sensibilisés aux techniques « d'ingénierie sociale » permettant de les subtiliser ou de les deviner.

Le cas échéant l'accès aux systèmes d'information ou des applications spécifiques ou encore l'exercice de fonctions de gestion de ressources informatiques peut être conditionné à une habilitation de défense.

5.1.2 - Charte informatique

La charte informatique du laboratoire est la charte informatique du CNRS (version du 2007) Cette charte est annexée au règlement intérieur du laboratoire et d'application obligatoire.

5.2 – Politique de sécurité des données

L'unité est dépositaire des données utilisées ou conservées par les moyens mis à la disposition de ses agents dans le cadre des missions qui leur sont confiées. Elle conçoit et met en œuvre les mesures nécessaires et suffisantes pour garantir leur disponibilité, leur intégrité et leur confidentialité, pour authentifier les utilisateurs et pour tracer leurs activités conformément à la politique de gestion des traces du CNRS.

⁶ Bien que la description de la procédure de gestion de compte n'ait pas à être détaillée dans ce document pour ne pas l'alourdir, il faudra la décrire par ailleurs précisément. Par exemple pour l'ouverture d'un compte : « la personne doit se présenter au secrétariat du directeur (c'est lui qui doit gérer le personnel non le service informatique -NDR) où il prendra connaissance des règles en vigueur (charte, PSSI, etc. -NDR) et signera un document comme quoi il en a effectivement pris connaissance. Le secrétariat transmet alors son visa au service informatique pour l'ouverture technique du compte ... etc. » Pour la fermeture : « le secrétariat ainsi que les responsables d'équipes informent le service informatique du départ d'une personne afin de clore le compte. Les données appartenant à ce compte sont alors transférées au responsable d'équipe ... etc. »

L'unité gère les procédures de chiffrement et de recouvrement des clés privées des utilisateurs⁷.

Le CSSI est « autorité d'enregistrement » pour les certificats CNRS délivrés dans l'unité⁸.

5.2.1 - Protection des données sensibles

Il est procédé régulièrement à un examen des données afin d'identifier celles présentant un caractère de sensibilité et de les repérer selon leur besoin de sécurité.

Les données sensibles font plus particulièrement l'objet d'une protection au niveau du contrôle d'accès, du traitement, du stockage, du transport ou de l'échange pour en assurer la confidentialité.

Le CSSI est responsable de la définition et du contrôle des procédures⁹ afférentes à cette protection particulière.

5.2.2 – Protection des données à caractère personnel

Les fichiers à caractère personnel font l'objet d'une procédure particulière en vue d'une déclaration ou d'une demande d'autorisation à la CNIL, du respect des finalités déclarées de leur traitement et d'une protection renforcée de leur contenu.

Le CSSI de l'unité, sous l'autorité du directeur, contribue à l'information et la sensibilisation des responsables de traitement. Il incite à la correction d'éventuelles anomalies et en cas de difficulté fait part des éventuels incidents à sa hiérarchie et à la chaîne fonctionnelle SSI.

Les données à caractère personnel constituent des données sensibles et comme telles doivent faire l'objet de protection.

5.2.3 - Politique de sécurité des postes de travail

Conformément à la charte utilisateur du CNRS, l'utilisation d'Internet pour un usage non professionnel est tolérée. Toutefois le personnel de l'unité n'est autorisé à utiliser à titre personnel sur Internet que les services de messagerie, de noms, de transfert de fichiers et de consultation de données en clair ou chiffrées¹⁰. Il ne doit mettre en place aucun service sur son poste de travail sans autorisation du CSSI¹¹ et avis des ASR.

L'activité sur les postes de travail est tracée et conservée conformément à la politique de gestion des traces du CNRS (les traces restent sur le poste).

⁷ Il n'est pas besoin ici d'en dire plus, les détails sont à mettre dans la documentation de la procédure à laquelle il est fait allusion.

⁸ L'unité a décidé d'utiliser les certificats CNRS (ce n'est évidemment pas le cas de tout le monde !)

⁹ Le référentiel SSI de l'unité doit comprendre la description précise des mesures permanentes prises pour :

- autoriser l'accès aux données et les droits de les modifier
- contrôler l'historique des accès
- contrôler l'historique des modifications
- respecter les règles en matière de protection spécifique
- isoler l'environnement de production.

Toutefois cette description n'est pas à intégrer dans la PSSI, seuls les principes et exigences de sécurité sont à préciser.

¹⁰ On élimine toute activité Internet indésirable (téléchargements illicites, Skype, etc.) en citant celles qui sont autorisées et en interdisant toutes les autres.

¹¹ Afin d'éviter la mise en place de serveurs non maîtrisés et les « peer 2 peer ».

Les machines sont administrées à partir d'un poste central. Sauf autorisation du CSSI et avis des ARS les utilisateurs n'ont pas les droits administrateurs sur leurs machines. Les machines qui ne sont pas administrées par le service informatique ont des accès limités au réseau du laboratoire¹².

Les postes de travail sont protégés contre les virus et les logiciels espions. Les flux de données sortant sont contrôlés par l'utilisateur¹³ et sa session de travail est verrouillée après 5 minutes d'inactivité.

Toute acquisition d'un logiciel doit faire l'objet d'une étude précisant ses caractéristiques de sécurité. Cette étude doit être approuvée par le directeur de l'unité ou, en son nom, le CSSI.

Les postes de travail dédiés aux partenariats industriels sont isolés logiquement¹⁴ du reste du réseau et leur accès physique est restreint aux personnels autorisés.

5.2.4 - Politique de sécurité des supports amovibles et des matériels nomades

Les supports amovibles et les disques durs des matériels portables sont systématiquement protégés au moyen d'un chiffrement de surface¹⁵.

L'unité met en place l'organisation permettant un recouvrement des clés privées¹⁶.

Une vérification du niveau de sécurité est effectuée avant l'accès au réseau d'un matériel nomade ou d'un support amovible.

La sortie et l'utilisation à l'extérieur de l'unité de tout équipement informatique appartenant à l'unité doit avoir été autorisée par le directeur de l'unité.

La connexion par des moyens nomades du CNRS au système d'information d'un tiers doit respecter les règles de sécurité de ce tiers.

5.2.5 – Politique de sécurité des serveurs

L'administration des serveurs de l'unité est sous la responsabilité de l'administrateur système et réseaux.

5.2.6 – Politique de sécurité des applications¹⁷

La sécurité est prise en compte à toutes les étapes d'un projet, interne ou externe, lié au système d'information de l'unité. Pour cela, un dossier de sécurité accompagne chaque projet et précise les enjeux, les méthodes, les mesures préconisées, les jalonnements et les tableaux de bord éventuels

Les applications informatiques de gestion et les applications Internet (Web, FTP, SSH, ...) sont sécurisées, en cohérence avec la sensibilité des informations traitées et échangées.

L'utilisation des applications de comptabilité et de gestion de l'unité est limitée aux personnels habilités.

Les flux du réseau de gestion administrative de l'unité sont protégés contre les écoutes¹⁸.

¹² Typiquement depuis le réseau « visiteur » ou « contrôle commande » on aura les mêmes possibilités d'accès aux ressources du laboratoire que depuis un FAI externe au laboratoire.

¹³ On pense ici à l'installation d'un pare-feu sur les postes de travail ...au moins Windows.

¹⁴ On pense ici soit à une connexion isolée physiquement du reste du réseau soit à des Vlan.

¹⁵ Dans cet exemple de PSSI, le choix de protection des données (essentiellement contre la perte ou le vol) des matériels amovibles et nomade est le chiffrement de surface. D'autres choix sont évidemment possibles.

¹⁶ Ceci sous entend la mise en place d'une organisation de recouvrement dans l'unité.

¹⁷ Pour toute autre situation particulière, se référer à la PSSI du CNRS §3.5 page 21.

Le courrier entrant est filtré pour éliminer au mieux les virus et les courriers non sollicités (Spam, Scam, etc.), la politique choisie est de n'éliminer que les messages fortement typés SPAM¹⁹ afin d'éviter la perte de message.

5.2.7 - Politique de sauvegarde, d'archivage et de restauration

Les données, à l'exception des données personnelles sont sauvegardées (sauvegardes totales ne permettant pas de recouvrer les dernières modifications de données, sauvegardes partielles permettant de recouvrer les données jusqu'à la veille au soir). Il est de la responsabilité des utilisateurs d'utiliser les espaces sauvegardés mis à disposition et de mettre en œuvre les facilités de synchronisation des données vers ces espaces pour les postes mobiles.

Leur stockage est sécurisé.

Certaines sauvegardes peuvent être archivées.

Le CSSI veille à ce que soient conservés les moyens de prouver l'ensemble des informations traitées, pendant la durée et sous la forme stipulé dans la politique de gestion des traces (à défaut d'exigences particulières, la durée de conservation des preuves doit être au moins égale aux prescriptions légales)²⁰.

Le CSSI vérifie que les techniques d'archivage utilisées offrent des garanties suffisantes de longévité et de lisibilité, compatibles avec la durée de conservation requise.

A la fin de la période de conservation, les opérations de destruction des archives sont traitées comme une activité de maintenance spéciale et appliquent les règles de sécurité prévues à cet effet.

Le retour à une situation normale et la restauration est garanti dans les 24 h en cas de dénis de service ou de perte de données²¹.

5.2.8 - Réparation, cession, mise au rebut des matériels de stockage

Avant tout envoi en réparation, cession ou mise au rebut d'un matériel, les données sont effacées au moyen d'un procédé efficace et selon les recommandations techniques nationales.

5.3 - Politique de sécurité réseau²²

5.3.1 – Politique de gestion du trafic sur les réseaux internes

Les différents flux réseau ne sont pas mélangés, en particulier sont isolés les flux suivants :

- les flux de données liés à l'administration de l'unité
- le réseau dédié aux visiteurs et congressistes
- le réseau dédié systèmes de pilotage du banc de test (contrôle commande)
- la DMZ qui contient l'ensemble des serveurs ouverts à l'extérieur
- le réseau de production de l'unité.

¹⁸ On pense au chiffrement de ce type de flux réseau.

¹⁹ Non-conformes aux RFC

²⁰ Il s'agit dans cet exemple de PSSI d'un exemple d'exigence d'assurance (idem pour l'item suivant).

²¹ Il s'agit là encore, d'un exemple d'exigence d'assurance correspondant à un objectif de sécurité particulier. Celle-ci n'est pas à généraliser : dans la plupart des cas, seul l'assurance de moyen est nécessaire.

²² Le directeur de l'unité assume tous les risques des choix technologiques des applications et des architectures systèmes (matériel et logiciel et réseau) déployées. Pour l'éclairer, le CSSI de l'unité lui soumet une analyse des risques (précisant explicitement les risques résiduels) qu'il doit approuver.

Entre ces réseaux et entre les différents sites de l'unité un pare-feu est mis en place qui effectue un filtrage sur les flux, les services et les IP.

Les réseaux internes sont protégés contre les intrusions, les écoutes ou les attaques provoquant des dénis de service.

Les mots de passe ne circulent pas en clair sur le réseau.

L'interconnexion réseau entre les sites de l'unité ne reste pas indisponible pendant plus de vingt-quatre heures ouvrées²³.

L'enregistrement des traces est centralisé sur un système ne permettant pas l'effacement de fichier.

5.3.2 - Politique d'accès à distance aux réseaux internes

Les accès à distance aux réseaux de l'unité sont authentifiés, chiffrés²⁴ et limités aux personnels autorisés. L'authentification des accès distants est individuelle.

Les ordinateurs utilisés pour les accès distants respectent les standards de l'unité pour les machines nomades. Cela signifie au minimum que l'ordinateur de l'utilisateur distant est protégé des virus et des malveillances du réseau (Internet, réseau hôte, etc.) et qu'il ne peut invalider ou modifier ces protections.

Tout vol ou incident de sécurité déclenche une procédure de modification de la protection des accès distants.

Un utilisateur distant connecté à l'unité ne peut permettre, consciemment ou non, à un tiers d'atteindre le réseau de l'unité.

Aucune ouverture session en provenance d'Internet n'est autorisée à atteindre directement le réseau interne de l'unité.

5.3.3 – Politique de sécurité des réseaux sans fil :

L'accès au réseau sans fil « labo » est autorisé à toute personne qui dispose du droit de se connecter et peut s'identifier/s'authentifier²⁵.

Les données émises en particulier les données d'authentification et les tunnels vers les autres réseaux du laboratoire ne peuvent être ni écoutées ni modifiées²⁶.

L'accès au réseau sans fil « visiteurs et congressistes » est soumis à une validation par un contact du laboratoire. Il ne donne pas accès aux ressources du laboratoire²⁷. Il ne permet pas d'ouvrir de service à l'extérieur et ne donne accès à l'extérieur que pour un nombre limité de protocoles²⁸.

L'utilisateur n'effectue sur ce réseau que des opérations ne nécessitant pas des accès à des informations sensibles.

²³ Il s'agit là encore, d'un exemple d'exigence d'assurance liée aux objectifs de sécurité spécifique de l'unité. D'autres unités n'auront pas forcément une telle exigence. Idem pour l'item suivant.

²⁴ Pour ne pas faire référence à une solution technique, on devrait dire « protégés contre les écoutes et les atteintes à l'intégrité » plutôt que chiffré ...

²⁵ Cela veut dire qu'une personne non autorisée ne doit pas pouvoir se connecter au réseau sans fil

²⁶ Cela veut dire utiliser WAP2 comme protocole de préférence au WEP, AES pour accéder aux autres réseaux.

²⁷ En pratique on aura les mêmes possibilités d'accès aux ressources du laboratoire que depuis un FAI externe au laboratoire

²⁸ Typiquement HTTP, HTTPS, DNS

5.3.4 - Politique d'accès à Internet depuis le réseau interne

Les transmissions²⁹ et les échanges d'informations ou de données sont soumis à la règle générale du contrôle dans les deux sens (émission/sortie et réception/entrée).

Les émetteurs et des destinataires sont identifiés et les identités sont authentifiées.

La surveillance des machines qui sont en relation directe avec Internet est assurée en permanence. L'établissement d'un standard associé à des procédures et des contrôles assure le respect de ce principe.

5.3.5 - Sécurité des infrastructures réseaux et télécoms

Les réseaux de télécommunication (y compris la téléphonie³⁰) sont gérés par le CRI de l'Université de Montcanin.

L'utilisation des téléphones sans fil est soumise à l'accord préalable du CSSI.

L'accès physique et logique aux équipements de l'infrastructure réseau est protégé

6) Dispositions diverses

6.1 - Procédure de traitement des incidents et plans de gestion de crise

La direction de l'unité est responsable de la coordination et de la mise en oeuvre du plan de traitement des incidents³¹, du plan de gestion de crise et du plan de retour à l'activité.

Le CSSI pilote et coordonne l'élaboration de ces plans de gestion des événements pouvant perturber les systèmes d'information ou plus généralement entraver la bonne réalisation des missions de l'unité.

Le CSSI est responsable de l'organisation d'un plan de contrôle régulier prévoyant la périodicité et la nature des tests à effectuer.

6.1.1 - Gestion d'incidents

Chaque acteur du SI, utilisateur ou administrateur est sensibilisé à l'importance de signaler tout incident réel ou suspecté.

Les avis des CERTs sont suivis et les correctifs appliqués sur les postes et les serveurs ouverts à l'extérieur.

²⁹ Le niveau de sécurité des réseaux doit être décidé pour répondre aux exigences de sécurité sur les « données ordinaires » qui y circulent, non pour celles des données les plus sensibles qui devront plutôt faire l'objet de procédures particulières.

³⁰ Si le PABX n'avait pas été géré par l'unité, on aurait écrit : « Le PABX est géré suivant le référentiel SSI du CNRS » (cf : http://www.sg.cnrs.fr/FSD/securite-systemes/documentations_pdf/securite_systemes/guide.pdf page 3)

³¹ On entend par « plan de traitement des incidents » l'ensemble des actions qui doivent être mises en oeuvre pour faire face à un incident de sécurité (causée par un sinistre, une malveillance, un accident ou une panne). Ce dernier plan est complété par un « plan de crise » lorsque l'incident est assez significatif pour être signalé (cf en annexes « le traitement des incidents de sécurité » et « le plan de crise »).

Des tests de vulnérabilité sur les postes de travail, les serveurs et le réseau sont effectués régulièrement.

Une détection d'intrusion est faite en temps réel.

Les incidents font l'objet d'une procédure de traitement et de signalement définie au niveau national.

La procédure de gestion des incidents est connue des administrateurs systèmes et réseaux, du CSSI et du directeur de l'unité afin de leur permettre de réagir à bon escient et de savoir à qui transmettre l'information.

Les vols d'ordinateurs ou de supports de données doivent être considérés comme des incidents de SSI et traités selon le même principe.

Le signalement des incidents à la chaîne fonctionnelle est systématique et relève de la responsabilité du CSSI.

Les données statistiques relatives à la gestion des incidents sont intégrées dans le tableau de bord de la SSI.

L'université de Montcanin, et l'ENSMC pour ce qui la concerne l'antenne de l'Ecole, sont tenus informés des incidents graves et leur avis est sollicité préalablement à tout dépôt de plainte.

6.1.2 - Gestion de crise

Le plan de gestion de crise du CNRS intègre les risques liés à l'informatique ainsi que les risques susceptibles d'une incidence sur la sécurité des systèmes d'information. Pour ces incidents, la chaîne fonctionnelle participe à la cellule de gestion de crise du CNRS.

Le FSD prévoit le dispositif organisationnel propre aux crises de nature informatique. Il doit être informé dès le déclenchement de toute crise ayant une incidence sur la sécurité des systèmes d'information. Il veille à la bonne information des autres structures concernées dont la cellule nationale de gestion de crise du CNRS.

6.1.3 - Plan de continuité

Sous la responsabilité du CSSI, l'unité définit un plan de continuité et les procédures correspondantes. Ce plan permet, dans un premier temps, de maintenir en mode dégradé les activités critiques, puis de récupérer et de restaurer toutes les fonctionnalités du système d'information.

6.2. - Maintien du niveau de sécurité

La mise à jour des systèmes, des applications et des « firmware » est effectuée suivant la procédure correspondante³².

Les dispositifs de sécurité sont testés.

³² Cette procédure est naturellement à définir et entre dans le référentiel de sécurité.

6.2.1 - Sensibilisation et formation des utilisateurs

La formation, la sensibilisation et l'information des différents acteurs, de l'expert SSI à l'utilisateur en passant par le responsable de l'entité sont cruciales pour la sécurité. Sous la responsabilité de la chaîne fonctionnelle SSI du CNRS, des actions en ce sens sont régulièrement menées au niveau local, régional et national.

En relation avec la chaîne fonctionnelle, le CSSI propose chaque année au directeur de l'unité des plans de formation sur la sécurité informatique à l'intention des administrateurs système et des différents types d'utilisateurs :

- Développement des applications, règles de programmation,
- Utilisation des moyens informatiques,
- Administration systèmes et réseaux,
- Réaction sur incident,
- Accueil des nouveaux entrants.

La sensibilisation se fait de manière permanente par les contacts étroits que le CSSI noue avec les personnels de l'unité. En outre il organise régulièrement sur des thèmes précis des séances de sensibilisation pour le plus large public possible.

Le CSSI participe activement aux formations délivrées régionalement.

6.2.2 - Posture de sécurité

En matière de sécurité des systèmes d'information, le niveau normal des recommandations faites dans le cadre de la politique interne de SSI correspond aux dispositions jaunes et orange du plan Vigipirate.

Ces recommandations sont rappelées régulièrement par le FSD via les délégations régionales du CNRS.

Les dispositions internes de sécurisation doivent permettre une réactivité suffisante en cas de passage au niveau rouge de mesures propres à la SSI.

Le plan d'intervention gouvernemental PIRANET fait l'objet annuellement d'exercices destinés à tester la réactivité de la chaîne d'intervention et la faisabilité des mesures préconisées.

6.2.3 - Mises en garde et recommandations de la chaîne fonctionnelle.

L'utilisation de certains matériels ou logiciels peut s'avérer préjudiciable à la sécurité des systèmes d'information. Ces produits font l'objet de « mises en garde » de la part de la chaîne fonctionnelle SSI, visant soit des recommandations d'utilisation, soit une interdiction pure et simple.

6.3. - Mesures du niveau effectif de sécurité

6.3.1 Contrôle de gestion de la SSI

La sécurité des systèmes d'information du CNRS fait l'objet de documents de cadrage, d'organisation et de planification. Le contrôle de gestion de la SSI s'opère sous la responsabilité du FSD. Il donne lieu à un tableau de bord de la SSI.

6.3.2 Audits

Le niveau de sécurité des systèmes d'information et la conformité de mise en œuvre des recommandations sur le terrain peuvent donner lieu à des audits externes, à des missions d'inspection (au sens de visite et échanges approfondis) réalisées par le CMSSI et à des autodiagnostic selon la méthodologie définie par le CNRS et mise en œuvre depuis plusieurs années.

6.3.3 Journalisation

Le SI comprend des dispositifs de journalisation, centralisée et protégée, de l'utilisation des services. L'objectif est de permettre de détecter des intrusions ou des utilisations frauduleuses, de tenter d'identifier les causes et les origines, d'éviter des contaminations d'autres sites par rebond et de remettre en place le système.

Le type et la durée de conservation (et donc de sauvegarde) des fichiers de traces à des fins de preuve est conforme à la politique de gestion des traces du CNRS.

Les utilisateurs sont informés des règles d'exploitation des fichiers de traces (contenu, durée de conservation, utilisation) dans le respect du « principe de proportionnalité » et des contraintes législatives et réglementaires concernant notamment le traitement des informations à caractère personnel.

Les fichiers de traces sont systématiquement analysés afin de repérer d'éventuels problèmes et de produire des statistiques et tableaux de bord.

6.3.4 Tableaux de bord

Un système d'indicateurs est conçu pour vérifier l'évolution de la SSI et aider à son pilotage.

6.4. - Maintenance et développement

6.4.1 - Télérations internes

Les interventions à distance sur les ordinateurs des utilisateurs par les personnes chargées de l'administration ou du support se font suivant les règles déontologiques de l'unité³³ et dans le respect des principes de la loi Informatique et Libertés.

6.4.2 - Infogérance et télémaintenance externes

Les prestations de maintenance font l'objet d'un contrat de sécurité précisant les obligations incombant aux prestataires :

- les règles de sécurité des opérations techniques
- les règles de sélection et de contrôle du personnel chargé des interventions
- les conditions d'accès aux bases de données
- les responsables à avertir en cas d'incident
- le cas échéant, les autres mesures de prévention ou d'organisation à mettre en œuvre, de part et d'autre, pour éviter les risques d'incident et l'aggravation de leurs conséquences.

³³ Cette charte déontologique est à élaborer sous la direction du directeur d'unité

En cas de nécessité les responsabilités seront imputées conformément aux clauses précisées de manière claire dans le contrat.

L'accès au système d'information de l'unité de la part de personnels d'entreprises extérieures est conforme à la politique générale d'accès aux moyens informatiques. Les obligations correspondantes, notamment la signature de la charte utilisateur, est mentionnée explicitement dans les dispositions contractuelles.

Un contrôle renforcé sur les ressources mises à disposition est effectué.

6.4.3 - Développement d'applications

Les modalités particulières relatives à la sécurité d'un projet ou d'un développement déterminé, sont décidées de commun accord entre le « *maître d'ouvrage* », le chef de projet et le CSSI.

Le contrat de sécurité est signé par tous les prestataires, internes comme externes, quels que soient les spécialistes ou les corps de métier.

Le CSSI contrôle les procédures d'utilisation et de conservation des contrats de sécurité.

6.4.4 - Clauses dans les marchés

Les marchés publics relatifs à des prestations informatiques (intégration de logiciels, infogérance, maintenance...) doivent comporter des clauses de confidentialité voire d'agrément et d'habilitation de personnes.

On se référera aux dispositions contractuelles types proposées par la chaîne fonctionnelle SSI.

6.5. - Référentiel SSI et gestion de la documentation SI

Le CSSI rédige et archive le rapport annuel sur l'état de la sécurité dans l'unité. Le rapport annuel comprend toujours un chapitre récapitulatif des accidents et dysfonctionnements sérieux et pour chacun d'eux, il fait une évaluation de leur impact et un bilan des leçons tirées, ainsi que les modifications apportées en conséquence aux moyens de prévention et aux stratégies de secours.

Les procédures de sécurité et les règles d'exploitation sont documentées

Les utilisateurs doivent être informés des mesures de sécurité des ressources informatiques auxquelles ils ont recours, de telle manière qu'ils puissent correctement évaluer les risques qu'ils supportent ou formuler leurs exigences supplémentaires. Le CSSI contrôle la constitution et la mise à jour de la documentation suffisante à cet effet.

Une veille technique et juridique est assurée au niveau national par le service du FSD, l'UREC et la DAJ pour la partie juridique ou la DSI pour les applications de gestion.

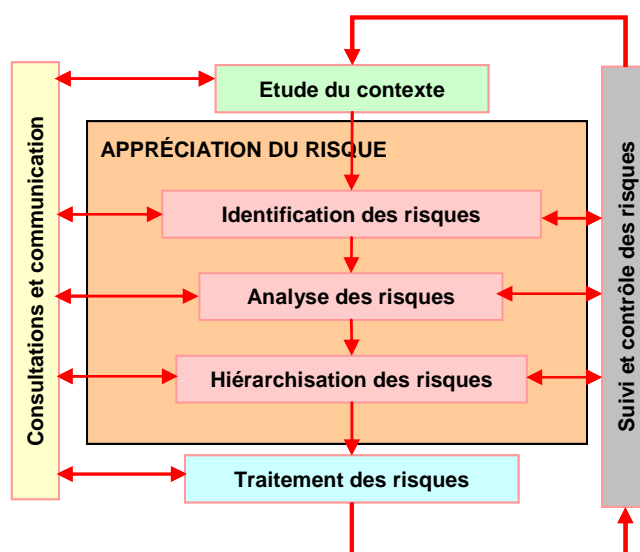
La gestion de la documentation SSI est assurée nationalement. La documentation comprend l'ensemble des dispositions législatives et réglementaires concernant la SSI, ainsi que l'ensemble des documents d'orientation nationale et les instructions et recommandations techniques propres au CNRS.

Annexe C

Gestion des risques en SSI : conseils de méthodologie

1) La gestion du risque

Commençons par faire la différence entre « analyse de risque » et « gestion du risque ». Dans l'ISO 31000 la gestion du risque est définie de la manière suivante :



Gestion du risque

L'appréciation du risque qui comprend :

- L'identification des risques
- L'analyse des risques
- La hiérarchisation des risques

n'est pas l'ensemble du processus de gestion du risque puisqu'il faut ajouter à celle-ci le traitement du risque, le suivi du risque et la communication sur le risque.

2) Recommandations préalables

La gestion des risques est un domaine largement exploré et il est inutile de prétendre redécouvrir ce qui a été déjà longuement étudié. Pour ce qui concerne les « systèmes d'information », il existe de nombreuses méthodes dont la plupart sont disponibles sur Internet³⁴.

Parmi les principales on citera la méthode EBIOS élaborée par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) et la méthode MEHARI mis en œuvre par le CLUSIF (Club de la Sécurité de l'Information Français)

Ces méthodes peuvent s'avérer lourdes et complexes si l'on souhaite les dérouler de bout en bout et s'attacher aux détails.

Par souci de simplicité et de cohérence, on recommandera donc :

- de s'appuyer sur un même vocabulaire (la terminologie unifiée devrait être publiée très prochainement dans le Guide ISO 73:2008),
- de s'appuyer sur une base de connaissance reconnue (nous proposons celle de EBIOS),
- de cibler le travail sur l'identification et l'évaluation des risques « propres à l'unité », l'évaluation (ou quantification sommaire) permettant de repérer des plages de priorité (à l'image de ce qui a été fait par le groupe de travail de gestion des risques du CNRS),
- dégager les spécificités et les priorités de l'unité afin d'adapter les risques déjà identifiés faisant partie du référentiel CNRS,

La détermination des objectifs et des exigences de sécurité au sein de l'unité n'est pas à faire comme si «on découvrait la SSI aujourd'hui », comme si le CNRS depuis plus de 10 ans n'avait pas déjà un référentiel, tant au niveau national (cf. les recommandations de l'UREC, les textes du service du FSD), qu'au niveau régional (cf. les formations et les sensibilisations qui ont été dispensées régionalement), mais aussi, souvent, au niveau des unités elles-mêmes. Nous n'avons pas à réinventer la roue chacun de notre côté !

Par exemple : on sait bien qu'il faut protéger la confidentialité des données à caractère personnel, que la disponibilité des services réseaux (particulièrement la messagerie) est importante, que l'intégrité des résultats scientifiques ne doit pas être mise en doute : des solutions de sécurité sont déjà préconisées, il n'est nul besoin de faire une étude lourde sur ces points si la spécificité de l'unité ne l'exige pas.

D'une manière plus précise, la PSSI du CNRS définit les enjeux, indique le périmètre d'une PSSI, présente les besoins au niveau de l'organisme, décrit l'organisation et les responsabilités, explique comment se coordonner avec les autres tutelles, donne des orientations de mise en œuvre et fixe les

³⁴ Par exemple :

- EBIOS : <http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html>
- MEHARI : <https://www.clusif.asso.fr/fr/production/mehari/>

principales lignes directrices. La PSSI d'unité doit décliner cette PSSI et les exigences de sécurité spécifiques par des règles opérationnelles, mais seules les situations spécifiques nécessitent une analyse de risque complète.

Celle-ci doit rester la plus pragmatique possible et être compréhensible par les utilisateurs – et la Direction –, a priori non spécialistes de ce type d'étude, de façon à obtenir leur participation à la démarche et ultérieurement leur adhésion. Pragmatique, cela veut dire avoir du bon sens et ne pas se laisser prendre au piège de la méthode (quand certaines valeurs déterminent les résultats finaux, la méthode n'est plus qu'un alibi !).

La gestion des risques impose un travail préalable d'identification des « éléments essentiels³⁵ » de l'unité et de leur besoin de sécurité en terme de confidentialité, intégrité et disponibilité (d'autres critères de sécurité peuvent encore être pris en compte, comme la traçabilité, la privacité, l'imputabilité, etc.)

Exemples : le laboratoire développe des technologies sensibles et particulièrement innovantes, l'activité du laboratoire conduit à de nombreux dépôts de brevets, on en déduira alors que la protection des données et résultats de travaux non encore couverts par un brevet est un souci majeur du laboratoire, et ce plus particulièrement pour tel département ou telle équipe. Les échanges réguliers et confidentiels avec tel partenaire industriel sont particulièrement à protéger, cette protection étant d'ailleurs imposée par le partenaire... On n'oubliera pas que des données bien que non scientifiques ou technologiques peuvent être très sensibles et imposer des protections (données nominatives de gestion du personnel, données médicales...).

Rappelons :

- que la démarche de gestion des risques est un travail d'équipe non celui d'un spécialiste au langage ésotérique.
- que la direction de l'unité doit valider les choix qui sont faits à chacune des étapes
- qu'il faut garder aux documents produits un caractère pédagogique et synthétique (ceux de l'étude, forcément analytiques, seront différents de ceux qui servent à la communication qui doivent être des synthèses).

³⁵ Un glossaire sur certains termes utilisés est disponible sur :

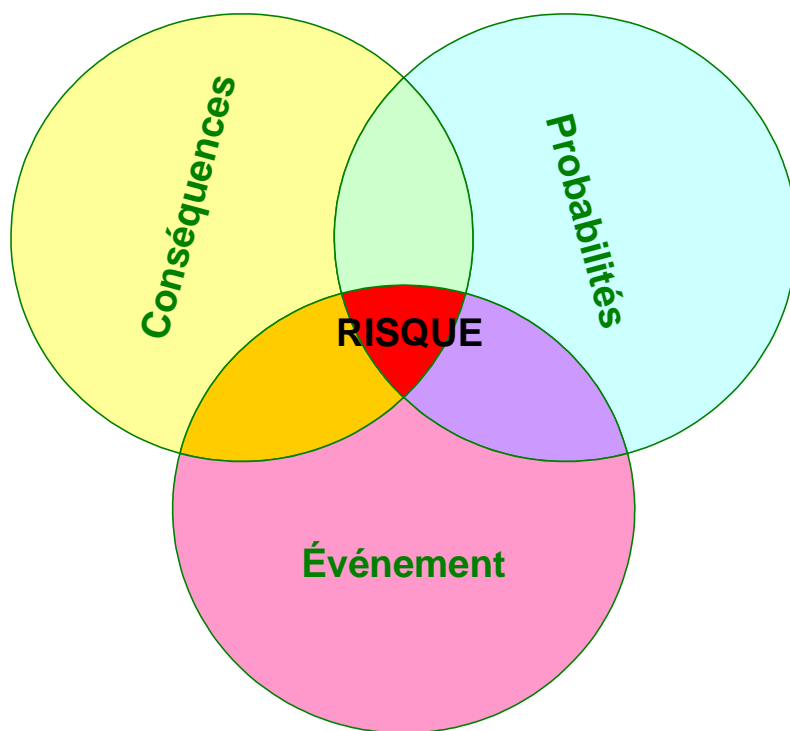
http://www.acfci.cci.fr/elections/Documents/Glossaire_Vote_electronique.pdf

Une introduction à la méthode EBIOS (avec son glossaire) est disponible sur :

<http://www.ssi.gouv.fr/fr/confiance/documents/methodes/ebiosv2-section1-introduction-2004-02-05.pdf>

2) Le risque en général

On confond souvent le concept de « risque » avec celui de « menace ». Pour lever toute ambiguïté, le Guide ISO 73 définit la notion de risque en général comme la **"combinaison de la probabilité d'un événement et de ses conséquences"**.



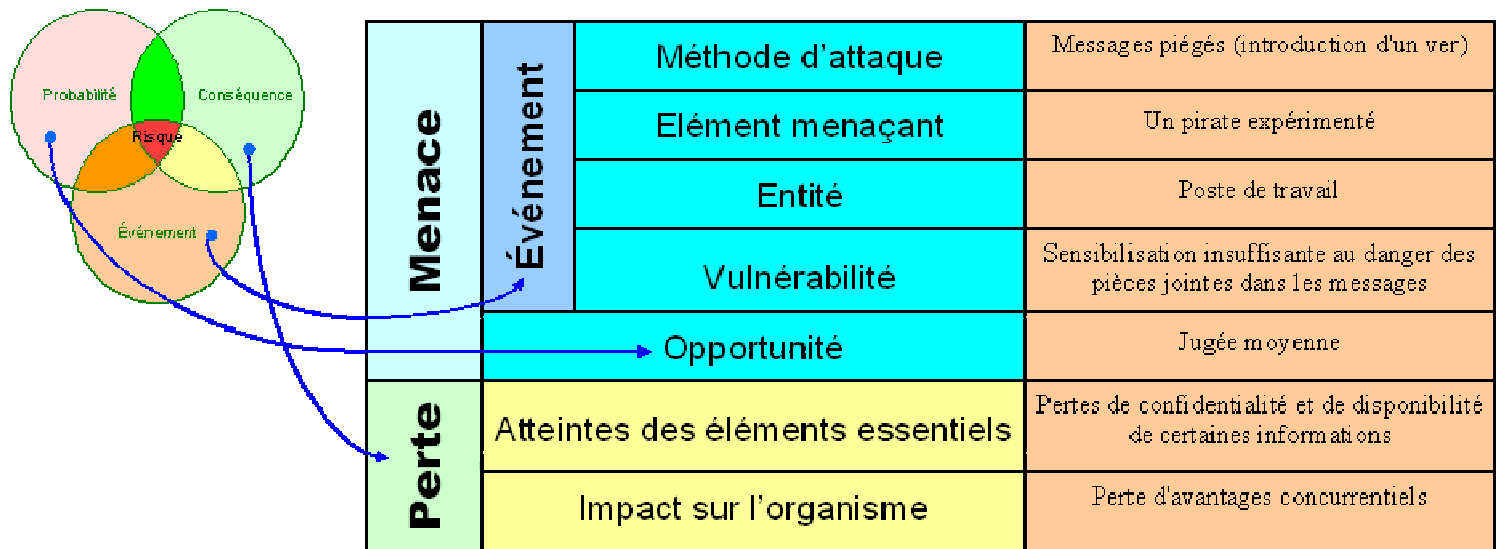
Par exemple, pour exprimer le risque pris par certaines banques en faisant des placements dans l'immobilier, il faut définir :

- un événement : « retournement de conjoncture dans l'immobilier »,
- une probabilité : « la possibilité d'un retournement de la conjoncture est envisageable »,
- des conséquences : « grosses difficultés financières pour certaines banques »

Ce risque s'exprimera donc de la façon suivante : « La conjoncture dans l'immobilier est incertaine, la possibilité d'un retournement est envisageable ; dans ce cas il faudra s'attendre à de grosses difficultés financières pour certaines banques qui ont investi une partie de leur portefeuilles dans ce secteur ».

3) Le risque en SSI

Les risques en SSI sont plus complexes et plus difficilement probabilisables. Certains d'ailleurs parlent « d'incertitude » plutôt que de probabilité. Dans EBIOS, il s'agit « d'opportunité ». Leur appréciation en est plus compliquée que la simple application de la définition générale. Aussi, la plupart des méthodes récentes décomposent-elles le risque plus subtilement :



Le risque dans EBIOS

1 - l'événement comprend :

- la méthode d'attaque ;
- l'élément menaçant ;
- l'entité vulnérable ;
- la vulnérabilité.

2 - la **probabilité** est souvent une « opportunité d'occurrence » (on a rarement en SSI des probabilités objectives). Événement et possibilité d'occurrence constituent « la menace ».

3 - les **conséquences** sont les pertes engendrées par un **besoin de sécurité** d'un **élément essentiel** non satisfait.

Avec les définitions suivantes pour les termes utilisés :

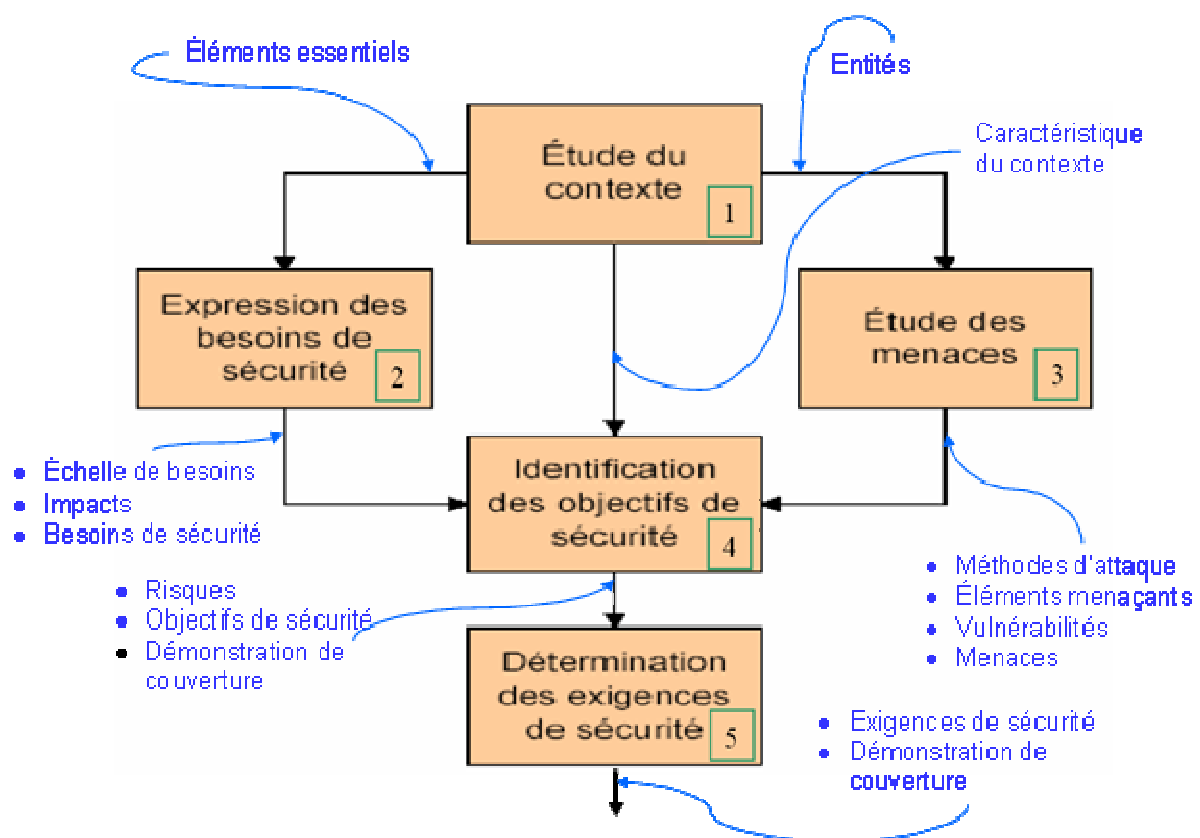
- **Éléments essentiels** (*Essential Element*) : les éléments essentiels sont les fonctions et les informations constituant la valeur ajoutée du système d'information pour l'organisme.
- **Entité** (*Entity*) : une entité est un bien qui peut être de type matériels, logiciels, système, réseaux, organisations, personnels et sites. Une attaque portant sur des entités impactera des éléments essentiels.
- **Élément menaçant** (Threat Agent) : un élément menaçant est une action humaine, un élément naturel ou environnemental qui a des conséquences potentielles négatives sur le système. Il peut donc être caractérisé par :
 - son *type* : naturel, humain, ou environnemental ;
 - sa *cause* : accidentelle ou délibérée.
 - dans le cas d'une cause accidentelle, il est aussi caractérisé par une exposition et des ressources disponibles ;
 - dans le cas d'une cause délibérée, il est aussi caractérisé par une expertise, des ressources disponibles et une motivation.
- **Vulnérabilité** (*Vulnerability*) : une vulnérabilité est la caractéristique d'une entité qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information.
- **Opportunité** (*Opportunity*) : une opportunité est la mesure de la possibilité de survenance d'une attaque.

- **Menace** (*Threat*) : c'est l'opportunité d'exploitation d'une vulnérabilité par un élément menaçant employant une méthode d'attaque.
- **Méthode d'attaque** (*Attack Method*) : une méthode d'attaque est le moyen type (action ou événement) pour un élément menaçant de réaliser une attaque.
- **Impact** (*Impact*) : l'impact est la conséquence sur l'organisme de la réalisation d'une menace.
- **Besoin de sécurité** : Le besoin de sécurité est la détermination précise et non ambiguë des niveaux correspondants aux critères de sécurité (*Sensitivity*) qu'il convient d'assurer à un élément essentiel. Les critères généralement utilisés sont :
 - la disponibilité : propriété d'accessibilité au moment voulu des éléments essentiels par les utilisateurs autorisés ;
 - l'intégrité : propriété d'exactitude et de complétude des éléments essentiels ;
 - la confidentialité : propriété des éléments essentiels de n'être accessibles qu'aux utilisateurs autorisés.

4) La gestion des risques dans une étude EBIOS

Fort de ces définitions, on peut enfin comprendre la formulation du risque SSI que donne EBIOS : « **le risque de sécurité des systèmes d'information** (*Information Security Risk*) est la combinaison d'une menace et des pertes qu'elle peut engendrer ». Cette nouvelle formulation a le mérite d'être plus concise mais l'inconvénient d'être absolument incompréhensible si on n'a pas en tête ce que recouvre ici « Menace » et « Pertes » (Cf. schéma ci-dessus)

L'étude se déroule alors de la manière suivante :



Cette manière de faire n'a plus à démontrer sa pertinence, elle a toutefois plusieurs inconvénients :

- Une étude EBIOS n'est pas un outil de communication : la forme très fortement analytique de l'étude, si elle est indispensable dans une première étape pour la perception et la classification des différents risques, rend très difficile la synthèse (une synthèse ne se contente pas de présenter des résultats, il faut aussi qu'elle les justifie). Or, l'analyse s'adresse aux « hommes de la technique » qui étudient, tandis que la synthèse aux « hommes du management » ... qui décident. Fournir un document de synthèse pour le management est donc indispensable pour la prise de décision.
- Pour garder un maximum d'objectivité à l'étude, il vaut mieux faire le choix des valeurs de « vulnérabilité » dont on tire « l'opportunité », le plus tard possible ... et en connaissance de cause. Pour établir rapidement la liste ordonnée de tous les risques de sécurité, une approche qualitative est d'ailleurs sans doute préférable à une étude quantitative.

5) Proposition de simplification de la méthode

Les méthodes, en général, s'appuient sur des « bases de connaissance » (listes des méthodes d'attaque, des entités, des vulnérabilités, etc.) qui permettent d'associer à chaque « élément essentiel » un ensemble de menaces et de vulnérabilités. La richesse de ces bases de connaissance permet de couvrir assez bien l'ensemble des risques. C'est plus particulièrement vrai pour EBIOS, dont nous recommandons fortement l'utilisation des bases de connaissance ... ce qui signifie : rester dans sa logique. Les simplifications envisagées ne peuvent alors se concevoir que dans le cadre de la méthode elle-même :

- Rester dans le cadre de la méthode EBIOS pour pouvoir utiliser sa base de connaissance, particulièrement pour faire le bilan des menaces et des vulnérabilités.

Mais :

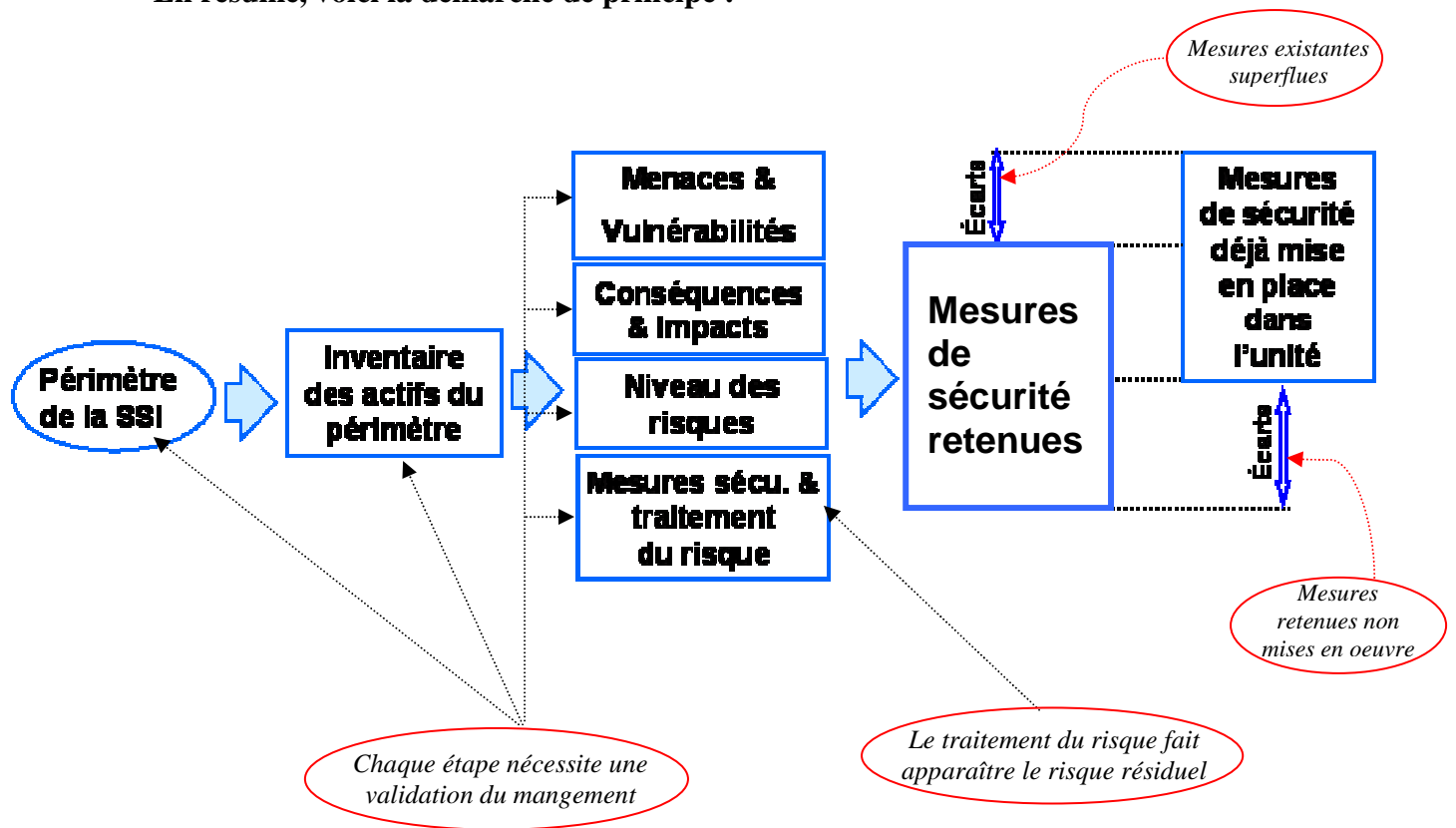
- Pour évaluer un risque il n'est nul besoin de donner une valeur artificielle au paramètre « opportunité », il suffit de rapprocher une vulnérabilité, des menaces identifiées en considérant pour chacune d'elle, la crédibilité des méthodes d'attaque, l'existence ou non d'éléments menaçant et l'atteinte aux besoins de sécurité qui en résulte. On en déduit alors facilement des « objectifs de sécurité » réalistes.
- Alléger au maximum l'étude du contexte pour aller rapidement à l'objet de l'étude.
- La démonstration de couverture n'est pas à faire (et par conséquent la justification des objectifs et des exigences de sécurité) : dans un processus d'amélioration continue de la sécurité (roue de Deming), cette étape n'est en général pas indispensable et la court-circuiter fait gagner en concision.
- Le management décide du niveau de sécurité en validant la valeur qu'il attache aux besoins (si possible au départ) et en validant in fine (ou non) les mesures de sécurité et en acceptant (ou non) les risques résiduels (là encore cette manière de faire permet de gagner un peu en concision par rapport à la méthode EBIOS).

Rappel : il convient de garder à l'esprit que

- l'analyse de risque s'inscrit dans un travail largement dégrossi au sein du CNRS et qu'un certain nombre d'éléments sont en facteur commun pour l'ensemble des unités
- la marge de manœuvre d'acceptation ou non des mesures par le manager est relativement étroite, compte tenu des choix prédéfinis au niveau national par le CNRS (les mesures nationales s'imposent sauf possibilité explicite de dérogation)

L'analyse de risque d'une unité n'est donc pas un exercice ex-nihilo mais doit s'opérer dans un contexte déjà prédéfini.

En résumé, voici la démarche de principe :



5) Conclusion

Cette démarche simplifiée permet d'obtenir une étude plus concise. Elle ne permet pas toutefois d'atteindre en exhaustivité et en rigueur EBIOS dans sa version « canonique », mais c'est un inconvénient moindre que celui d'un document trop analytique pour permettre une prise de décision par le management. En effet, dans une démarche d'amélioration continue de la SSI qui se donne les moyens de corriger et d'affiner en permanence la politique de sécurité, il y a de la place pour des approximations de ce type si elles permettent d'amorcer la roue de Deming.