L'ARCHITECTE-RÉFÉRENT EN SÉCURITE DES SYSTÈMES D'INFORMATION

L'objectif de ce document est de définir les compétences de l'architecte référent en sécurité des systèmes d'information, ou « ARSSI », par le biais d'un référentiel métier. Ce référentiel peut notamment être utilisé pour définir des formations adéquates ou autoévaluer son niveau de qualification et de pratique.

Introduction

L'ubiquité des technologies informatiques, l'interconnexion croissante des systèmes d'information ou encore l'affaiblissement du cloisonnement entre les sphères privées, publiques et professionnelles des utilisateurs posent aujourd'hui de nombreux défis dans le domaine de la cybersécurité.

Assurer la protection et la défense d'un système d'information nécessite de mettre en œuvre un ensemble de mesures de natures et de complexités variées pouvant reposer sur des dispositifs techniques et organisationnels. Un grand nombre de mécanismes, outils, démarches, méthodes et normes ont été développés, performants mais souvent complexes. Il est devenu indispensable de disposer de professionnels généralistes capables de comprendre les grands domaines des systèmes d'information et leur sécurité.

Dotés de compétences avancées, ces professionnels doivent aussi savoir réagir aux évolutions des systèmes et des menaces. Au-delà des spécialistes maîtrisant un domaine bien précis de la sécurité des systèmes d'information, ces généralistes doivent être capables d'appréhender dans son ensemble la sécurité d'un système d'information complexe, et dans toutes ses dimensions – technique, organisationnelle, juridique – afin d'en maîtriser la cohérence et l'efficacité de manière globale.

Rôle de l'architecte référent

L'ARSSI a pour vocation de garantir la sécurité des systèmes d'information tout au long de leur cycle de vie, en intervenant aux différentes étapes, depuis l'expression de besoin jusqu'à son retrait de service, en passant par le développement et l'exploitation.

Il est en particulier capable d'exercer les activités suivantes :

- formaliser les besoins de sécurité en prenant en compte toutes les dimensions ;
- élaborer des dispositifs techniques de sécurité répondant à des besoins de sécurité, en relation avec des experts techniques ;
- estimer ou faire estimer le niveau de sécurité d'un dispositif ou système d'information ;
- gérer la sécurité d'un système d'information – notamment en réagissant aux incidents de sécurité pendant la phase d'exploitation, pour en réduire les impacts.

L'ARSSI est doté d'un esprit critique et curieux afin qu'il soit capable, si nécessaire, de remettre en cause de manière pertinente et justifiée des propositions techniques et d'élaborer des alternatives crédibles.
Par l'étendue de ses compétences et de ses connaissances, par sa compréhension des dispositifs de sécurité, il est capable de coordonner les spécialistes SSI et de faire une synthèse de leurs travaux.
L'ARSSI joue également le rôle de médiateur entre des interlocuteurs ne connaissant que peu ou pas la SSI et des spécialistes de la SSI. Par sa pédagogie, il assure une meilleure prise en compte des besoins de sécurité, des risques et de leurs impacts, et une meilleure compréhension des mécanismes de sécurité mis en œuvre et de leurs conséquences.

L'ARSSI peut notamment exercer les fonctions suivantes :

- responsable SSI au niveau d'une direction ;
- responsable d'une équipe de spécialistes SSI (audit, projet, etc.) ;
- conseiller auprès des autorités et des chefs de projet.

Référentiel métier de l'ARSSI

Le tableau suivant précise les compétences et objectifs associés attendus.

	Connaître et formaliser les besoins de sécurité
1	Être conscient des enjeux de la sécurité et prendre en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire) de la problématique SSI.
2	Être capable de mener, de manière formelle, l'analyse d'un projet relatif à un système d'information complexe afin d'identifier les besoins en sécurité, les menaces et les risques, et d'en déduire les objectifs de sécurité.
3	Être capable de conseiller ou de convaincre un donneur d'ordre (autorité, chef de projet, DSI…) dans le domaine de la SSI.
	Élaborer un dispositif technique correspondant aux besoins de sécurité
4	Comprendre les problématiques de sécurité, notamment connaître et savoir identifier les risques liés à un système d'information (par domaine ou de manière globale).
5	Comprendre les forces et faiblesses des produits de sécurité, notamment ceux mettant en œuvre des mécanismes cryptographiques.
6	Être capable de définir une solution technique pour défendre un système d'information selon les grands axes de la défense en profondeur.
7	Être capable de faire des recommandations relatives à la SSI auprès d'un spécialiste technique d'un système d'information.
	Savoir estimer ou faire estimer le niveau de sécurité d'un dispositif
8	Estimer soi-même le niveau de sécurité d'un système d'information.
9	Connaître les différentes modalités d'un audit et savoir le préparer.
10	Savoir prendre en compte les résultats d'un audit, élaborer et conduire un plan d'action.
11	Savoir établir une démarche d'homologation et bien la conduire.
	Gérer la sécurité d'un système d'information
12	Être un interlocuteur auprès des acteurs du projet, des spécialistes informatiques, des administrateurs et des RSSI.
13	Maintenir le niveau de sécurité du système d'information, adapté aux contraintes métier.
14	Savoir formaliser les documents SSI.
15	Savoir veiller sur les dernières vulnérabilités, menaces et produits de sécurité et savoir les analyser.
16	Évaluer les impacts d'une vulnérabilité ou d'une menace.
17	Savoir détecter et gérer un incident de sécurité.

Complément au référentiel métier

Les lignes qui suivent ont pour but de détailler quelques éléments relatifs aux compétences et objectifs d'un ARSSI. Il s'agit bien ici de décrire les capacités attendues (savoir, savoir-faire, savoir être) et non pas de décrire l'ensemble des fonctions et missions que tout ARSSI doit assumer.

- Connaître et formaliser les besoins de sécurité –

1 Être conscient des enjeux de la sécurité et prendre en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire) de la problématique SSI.

- Maîtriser et savoir expliquer clairement les principes fondamentaux de la SSI et les vocabulaires employés.

L'ARSSI maîtrise notamment les notions de biens sensibles, critères de sécurité (confidentialité, intégrité, disponibilité), menaces, vulnérabilités, risques, objectifs de sécurité, défense en profondeur, etc.

- Acquérir et maintenir une vision correcte de la situation de la SSI au niveau international, étatique et industriel et l'intégrer dans ses problématiques propres.

L'ARSSI connaît les enjeux de la SSI, les grandes préoccupations des États et des industriels, les principales orientations stratégiques et industrielles dans le domaine.

- S'informer des orientations en termes de menaces et d'exploitation de vulnérabilités.

L'ARSSI sait analyser les rapports les plus pertinents en termes de SSI, les comprendre et en tirer bon usage. Il connaît en particulier les menaces et les vulnérabilités propres à son organisme d'appartenance ou aux systèmes d'information dont il a la charge.

- Connaître et prendre en compte les contraintes humaines, organisationnelles, techniques propres à son environnement.

L'ARSSI connaît, comprend et prend en compte les impératifs de son organisme en termes d'objectifs métier, les limites en ressources (humaines, budgétaires, organisationnelles, etc.), les contraintes environnementales.

- Identifier le contexte juridique d'un système d'information selon la nature des informations traitées.

L'ARSSI prend également en compte dans sa démarche les contraintes résultant de la législation et la réglementation. Il dispose pour cela d'un référentiel adapté à ses besoins et connaît ses interlocuteurs dans le domaine juridique.

- S'intégrer efficacement dans l'organisation SSI de son environnement.

L'ARSSI connaît ses interlocuteurs dans les différentes chaînes SSI existantes, leurs rôles, leurs responsabilités et s'intègre à cette organisation afin d'y collecter des informations, des conseils, voire des recommandations ou au contraire pour y apporter son expertise.

2 Être capable de mener, de manière formelle, l'analyse d'un projet relatif à un système d'information complexe afin d'identifier les besoins en sécurité, les menaces et les risques, et d'en déduire les objectifs de sécurité.

- Connaître la démarche générique de l'analyse de risque.

L'ARSSI connaît notamment les normes du domaine, les difficultés inhérentes à la démarche, la multiplicité et les limites des méthodes actuelles.

- Utiliser une méthode d'analyse de risque.

L'ARSSI maîtrise une méthode d'analyse de risque et il est aussi capable de s'approprier d'autres méthodes selon les exigences des employeurs ou des maîtrises d'œuvre.

- Appliquer de manière pertinente une méthode d'analyse de risque sur tout système.

L'ARSSI adapte sa méthode selon son niveau d'expérience, la complexité du système à étudier, les contraintes de temps et de disponibilité des acteurs. Il se détache du formalisme de la méthode pour parvenir à des résultats pertinents selon les délais imposés. Il sait aussi contrôler la qualité d'une analyse de risque et porter un jugement critique et constructif.

- Intégrer les acteurs d'un projet dans une analyse de risque.

L'ARSSI fait intégrer les acteurs du projet dans son analyse de risque, sait leur expliquer la démarche selon leur degré de compréhension, les conseille et leur apporte un appui efficace.

- Formaliser, au bon niveau, les résultats de l'analyse.

L'ARSSI rédige ou valide les documents formels issus de l'analyse de risque d'un système (expressions des objectifs de sécurité, cibles de sécurité, etc.). Il porte un regard critique sur l'analyse de risque et les réponses apportées.

- Prendre en compte l'aspect évolutif de l'analyse de sécurité.

L'ARSSI se tient informé des principales modifications apportées à un système d'information et adapte en conséquence l'analyse de risque associée.

3 Être capable de conseiller ou de convaincre un donneur d'ordre (autorité, chef de projet, DSI…) dans le domaine de la SSI.

- Comprendre le besoin de ses interlocuteurs, tant au niveau métier que technique.

L'ARSSI s'approprie le vocabulaire de son environnement, les enjeux et les processus. Il s'intègre dans le milieu métier auquel il apporte son expertise. Il traduit les besoins métier en termes de sécurité. Il est aussi

au contact des DSI et apporte son expertise dans la conduite des projets. Il intègre dans son analyse leurs besoins spécifiques.

- Se mettre au niveau de ses interlocuteurs.

L'ARSSI adapte son vocabulaire à son interlocuteur, lui expose ses idées et ses arguments de manière compréhensible et claire, selon son niveau de compétence et de disponibilité. Il adapte la présentation des mesures de sécurité à leur niveau de maturité.

- Sensibiliser les donneurs d'ordre.

L'ARSSI sensibilise les décideurs sur les enjeux de la SSI selon leur domaine de compétence et de connaissance de la problématique.

- Être mesuré et progressif.

L'ARSSI propose des solutions progressives et adaptées au risque analysé et à l'environnement : il ne recherche pas la solution parfaite mais tend à améliorer le niveau de sécurité du système d'information et la maturité des acteurs.

- Convaincre.

L'ARSSI propose des solutions cohérentes en apportant des arguments valables et solides, prenant notamment en compte tous les aspects de la SSI (droit, règlement, technique, etc.). Il s'appuie sur des références et sa compétence est reconnue. Il veille à entretenir des relations de confiance avec ses interlocuteurs. Il veille à présenter ses propositions, non sous la forme de contraintes, mais comme des solutions satisfaisant aux besoins opérationnels. Il fait adhérer les acteurs à la démarche SSI.

- Élaborer un dispositif correspondant aux besoins de sécurité –

4 Comprendre les problématiques de sécurité, notamment connaître et savoir identifier les risques liés à un système d'information (par domaine ou de manière globale).

- Maîtriser les concepts et principes de fonctionnement des systèmes informatiques (systèmes d'exploitation, réseaux, applications, bases de données, etc.).

L'ARSSI comprend et maîtrise les concepts et principes mis en œuvre dans un système informatique, tant au niveau système que réseau, et en saisit toute la portée technique dans le domaine de la sécurité. Ses connaissances lui permettent d'approfondir certains points, lorsque cela est nécessaire.

- Comprendre une architecture complexe.

L'ARSSI est capable d'étudier et d'analyser une architecture complète d'un système d'information complexe en prenant en compte toutes les composantes pertinentes pour la sécurité.

- Être capable de porter un regard critique sur un système ou sur un composant d'un système.

L'ARSSI saisit les enjeux de sécurité d'un système informatique. Il pose les questions pertinentes à ses interlocuteurs, chefs de projet ou techniciens par exemple, et peut vérifier et exploiter les réponses apportées. Il a la capacité d'apporter un regard critique et de remettre en cause les certitudes infondées.

- Identifier les risques d'un système informatique et y associer des besoins de sécurité.

L'ARSSI identifie les vulnérabilités réelles et les menaces spécifiques à un système informatique. Il évalue les impacts des risques associés de manière pratique. Il contribue à la recherche de solutions adaptées pour traiter ces risques, tant en termes techniques qu'organisationnels, selon le niveau de maturité et les contraintes des acteurs concernés. Il est en contact avec des spécialistes pour apporter la solution la plus adaptée.

5 Comprendre les forces et faiblesses des produits de sécurité, notamment ceux mettant en œuvre des mécanismes cryptographiques.

- Comprendre les principes des mécanismes des produits de sécurité dans le domaine de la sécurité informatique et de la cryptographie, et si nécessaire dans la lutte des signaux compromettants.

L'ARSSI comprend les besoins associés, les concepts employés, les différentes méthodes pour les mettre en œuvre. Il sait manipuler les concepts sans cependant être formé pour paramétrer ou configurer les produits de sécurité. Il comprend impérativement les concepts de la cryptographie symétrique et asymétrique, les propriétés des fonctions de hachage, les principes des infrastructures de gestion de clés (IGC) ou encore la notion de garantie de préservation de la confidentialité dans le futur (PFS).

- Connaître les différents produits de sécurité et leurs conditions d'emploi.

L'ARSSI connaît les différentes solutions et technologies de sécurité, et remet régulièrement à jour ses connaissances. Il comprend les objectifs et services apportés par ces technologies, connaît leurs modalités d'emploi et veille à les faire respecter. Lorsqu'elles ne sont pas respectées, il identifie les risques résultant, les évalue et les fait connaître aux responsables concernés, en proposant le cas échéant des mesures correctives ou palliatives.

- Identifier les limites de tels mécanismes, notamment dans leurs conditions d'emploi.

L'ARSSI connaît les principales vulnérabilités relatives aux principes et aux technologies employées dans les dispositifs de sécurité et les différentes méthodes d'attaque associées. Il sait porter un regard critique sur une solution de sécurité, notamment dans le cadre de sa mise en œuvre.

- Identifier les contraintes humaines, organisationnelles et techniques des produits de sécurité.

Dans son analyse, l'ARSSI prend en compte l'environnement dans lequel sont déployés les produits de sécurité.

- Comprendre un agrément, une certification.

L'ARSSI connaît les différentes formes de labellisation (niveaux d'agrément et de certification notamment), et leurs modalités. Il sait les apprécier et les exploiter de manière pertinente.

6 Être capable de définir une solution technique pour défendre un système d'information selon les grands axes de la défense en profondeur.

- Comprendre et savoir appliquer les principes de la défense en profondeur.

L'ARSSI connaît et sait mettre en œuvre les principes de la défense en profondeur sur tout système d'information en fonction des besoins de sécurité, selon les 5 grands axes (prévenir, bloquer, limiter,

détecter, réparer). Il sait expliquer ces principes et proposer pour leur mise en œuvre des solutions adaptées aux contraintes.

- Proposer une solution adaptée aux contraintes et aux besoins, propre à l'environnement dans lequel elle sera déployée.

L'ARSSI propose des solutions sécurisées cohérentes et adaptées au système d'information et aux besoins de sécurité, privilégiant notamment les produits labellisés. Il identifie et présente les risques résiduels. Cette proposition s'appuie sur une analyse de risque, sur la maturité et les compétences réelles des acteurs du système. Il inclut dans ses solutions l'aspect organisationnel et le volet formation. Il préconise enfin une politique de sécurité propre au système.

- Connaître les référentiels et savoir les adapter.

Dans son analyse, l'ARSSI s'appuie sur des référentiels reconnus, notamment sur des guides et des recommandations, tout en les adaptant aux contextes du système d'information. En relation avec les techniciens, il analyse les conséquences des modifications apportées et en évalue les risques. Il peut aussi apporter son expertise auprès des rédacteurs des guides de recommandations.

- Prendre en compte la notion de maintien en condition de sécurité (MCS).

Dans toutes ses propositions, l'ARSSI prend en compte le maintien en condition de sécurité (MCS) dans le cadre des évolutions du système informatique (corrections, modifications, migrations, obsolescences, etc.) et des besoins tant métier que techniques. Ses propositions incluent des recommandations pour garantir le MCS.

7 Être capable de faire des recommandations relatives à la SSI auprès d'un spécialiste technique d'un système d'information.

- Comprendre les métiers des spécialistes techniques d'un système d'information.

Sans chercher à se substituer à eux ou tenter d'égaler leur compétence, l'ARSSI connaît l'environnement de travail, les difficultés et les contraintes des spécialistes techniques.

- Améliorer l'hygiène informatique des administrateurs.

L'ARSSI évalue le niveau de maturité des administrateurs en termes de SSI. Il veille à diffuser les bonnes pratiques et à contrôler leur application.

- Apporter une réponse adaptée aux besoins de sécurité.

L'ARSSI apporte son expertise pour maintenir ou améliorer le niveau de sécurité des systèmes information. Il propose aux spécialistes techniques des solutions répondant aux besoins de sécurité bien identifiés. Il cherche leur adhésion. En cas d'absence de réponse satisfaisante, il se met en relation avec des spécialistes SSI.

- Faire appliquer de manière pertinente les référentiels.

L'ARSSI assure la promotion des référentiels reconnus et pertinents – par exemple les guides et les recommandations – auprès des acteurs concernés. Il fait contrôler leur application et fait justifier toute déviation pour juger de leur pertinence et évaluer les risques induits.

- Estimer ou faire estimer le niveau de sécurité d'un dispositif -

8 Estimer soi-même le niveau de sécurité d'un système d'information.

- Contrôler régulièrement l'application de la politique de sécurité en vue d'identifier les vulnérabilités et les risques associés.

L'ARSSI sait réaliser un état des lieux des mesures organisationnelles et techniques définies dans la politique de sécurité, soit en les contrôlant directement, soit en les faisant contrôler, généralement sur la base d'un référentiel et dans le respect de la législation et la réglementation. Il en déduit un niveau de sécurité du système d'information. Il peut utiliser les outils classiques d'audit technique et en exploiter les résultats, et connaît les points les plus critiques devant être contrôlés prioritairement.

- Évaluer un niveau de sécurité à partir d'indicateurs.

A partir d'un ensemble d'indicateurs, de comptes rendus d'incidents ou d'anomalies, l'ARSSI identifie d'éventuelles vulnérabilités ou attaques et le cas échéant approfondit les investigations pour les confirmer ou les préciser.

- Connaître les méthodes et les principaux outils d'audit.

L'ARSSI connaît les principaux outils d'audit, par exemple permettant la cartographie des réseaux ou l'identification de vulnérabilités, et peut en exploiter les résultats. Il connaît leurs limites et leurs effets sur le fonctionnement du système, ainsi que le contexte juridique ou réglementaire dans lequel ils peuvent être mis en œuvre.

9 Connaître les différentes modalités d'un audit et savoir le préparer.

- Définir les enjeux précis d'un audit en relation avec les acteurs du système d'information et choisir le type d'audit approprié.

L'ARSSI fait préciser les objectifs attendus d'un audit par rapport au cadre dans lequel cet audit est effectué (homologation, certification, vérifications suite à une évolution, soupçons de malveillance, état des lieux d'un système inconnu, etc.). À partir des objectifs fixés, il propose à l'autorité responsable un type et un périmètre d'audit et les fait valider.

- Diriger, en relation avec les auditeurs, la préparation de l'audit.

L'ARSSI identifie avec précision le type attendu de prestations, les cibles pertinentes, les référentiels à privilégier, répertorie la documentation utile et définit les modalités pratiques de l'audit. Il informe les auditeurs de la sensibilité de la cible, des contraintes réglementaires et professionnelles. Il fait valider aux autorités responsables le contrat d'audit.

- Veiller au bon déroulement de l'audit.

L'ARSSI vérifie le respect du contrat d'audit, répond aux demandes des auditeurs, réagit en cas d'incident, et prépare avec les auditeurs les éléments de restitution.

10 Savoir prendre en compte les résultats d'un audit, élaborer et conduire un plan d'action.

- Comprendre les résultats d'un audit.

L'ARSSI est capable de comprendre le compte-rendu d'un audit et de l'approfondir, si nécessaire, avec l'aide des auditeurs. Il peut demander des précisions et leur apporter son expertise.

- Exploiter les résultats d'un audit.

En adoptant le recul nécessaire, l'ARSSI interprète les résultats d'un audit en fonction du type d'audit et en prenant en compte le contexte du système d'information. Il propose un plan d'action pertinent et réaliste, en précisant notamment des priorités de traitement en fonction de la criticité et de la facilité de mise en œuvre des mesures. Il fait préciser les responsabilités et le calendrier, puis assure le suivi des actions et des points de contrôle.

11 Savoir établir une démarche d'homologation et bien la conduire.

-

- Comprendre et faire comprendre les enjeux de l'homologation.

L'ARSSI connaît les principes et les modalités d'une démarche d'homologation. Il sensibilise et implique les acteurs concernés en s'assurant de la bonne compréhension de la démarche et des enjeux.

- Établir une stratégie d'homologation.

Selon la nature du système d'information et son contexte notamment juridique et réglementaire, l'ARSSI établit ou fait établir une stratégie d'homologation en précisant notamment le périmètre, les responsabilités, les référentiels et les modalités. Il vérifie en particulier sa pertinence et sa faisabilité, avant de la faire valider par l'autorité responsable.

- Diriger la démarche d'homologation.

L'ARSSI conduit ou fait conduire la démarche d'homologation établie, en relation avec l'ensemble des acteurs. Il rend compte régulièrement à l'autorité d'homologation du suivi de la démarche et des risques de dysfonctionnement ou d'échec.

- Préparer la commission d'homologation sous la présidence de l'autorité d'homologation.

L'ARSSI met en place la commission, réunit les acteurs et apporte son expertise en ayant soin de conserver son objectivité.

- Gérer la sécurité d'un système d'information –

12 Être un interlocuteur auprès des acteurs du projet, des spécialistes informatiques, des administrateurs et des RSSI.

- Apporter son expertise aux acteurs du système d'information.

L'ARSSI aide à concevoir un système d'information prenant en compte les besoins de sécurité, puis à améliorer son niveau de sécurité ou à le maintenir. Il propose des solutions, évalue et valide les choix, et fait appel quand nécessaire à l'assistance d'entités spécialisées en SSI.

- Veiller à la prise en compte de la sécurité dans un projet dès sa conception.

L'ARSSI veille à la prise en compte de la SSI dès les phases initiales d'un projet, en relation avec le chef de projet et le RSSI de l'organisme. Il participe aux différentes phases d'un projet et garantit la satisfaction des besoins de sécurité qu'il a contribué à faire exprimer.

13 Maintenir le niveau de sécurité du système d'information, adapté aux contraintes métier.

- Sensibiliser les acteurs de projet sur les enjeux de MCS.

L'ARSSI sensibilise les différents acteurs aux enjeux de la maîtrise de la sécurité du système d'information dans la durée.

- Suivre l'évolution du système d'information dans la durée.

L'ARSSI se tient informé des modifications apportées au système d'information, notamment organisationnelles, qui peuvent remettre en cause sa sécurité. En cas de dégradation, il évalue les risques, propose des mesures et décrit les risques résiduels. Il en informe les responsables et peut le cas échéant proposer la suspension de l'homologation.

- Veiller au maintien de condition de sécurité.

L'ARSSI s'assure que les vulnérabilités associées à un système d'information sont couvertes par des correctifs techniques ou organisationnels. Il fait mettre en place un suivi des correctifs et fait contrôler leur application.

14 Savoir formaliser les documents SSI.

- L'ARSSI rédige ou fait rédiger les différents documents SSI (expressions des objectifs de sécurité, cibles de sécurité, procédures d'exploitation de sécurité, politiques SSI, plans d'actions, documents d'homologation, etc.). Il contrôle et valide ces documents avant de les faire approuver par les responsables concernés.

15 Savoir veiller sur les dernières vulnérabilités, menaces et produits de sécurité et savoir les analyser.

- Prendre connaissance régulièrement des vulnérabilités et de leur criticité.

L'ARSSI connaît l'état de l'art des vulnérabilités dans ses domaines de responsabilités, et des moyens de s'en prémunir, notamment en suivant les publications des CERT, et s'assure qu'ils soient connus des acteurs concernés. Il sait récupérer et exploiter les informations pertinentes d'un bulletin ou d'un avis de sécurité. En cas de risques avérés et en l'absence de correctif, il propose des solutions provisoires en relation avec les responsables métier et techniques.

- Être au courant de l'actualité SSI.

L'ARSSI s'assure de disposer des dernières informations pertinentes dans le domaine de la SSI, notamment dans le cas d'attaques informatiques d'ampleur (infections par exemple) ou encore à l'apparition de nouvelles solutions de sécurité. Il étudie les impacts sur les systèmes d'information de son domaine de responsabilité et propose, si nécessaire, des mesures préventives.

16 Évaluer les impacts d'une vulnérabilité ou d'une menace.

- Évaluer la gravité d'un événement redouté.

Lorsqu'il prend connaissance d'une vulnérabilité, l'ARSSI est capable d'identifier et d'analyser les impacts sur les systèmes d'information de son domaine de responsabilité et d'en évaluer la criticité réelle.

- Évaluer la pertinence d'une menace.

Informé d'une menace, l'ARSSI sait en évaluer la vraisemblance en prenant notamment en compte l'état de sécurité du système d'information.

- Informer les responsables.

L'ARSSI informe et implique au plus tôt sa hiérarchie en cas d'incident, en identifiant les risques encourus. Il précise les faits et informe sa hiérarchie des mesures à mettre en place.

17 Savoir détecter et gérer un incident de sécurité.

- Prévoir la remontée des incidents.

L'ARSSI s'assure de la mise en œuvre d'un dispositif technique et organisationnel permettant de détecter incidents et anomalies et de remonter aux personnes adéquates les signalements au travers d'une chaîne d'alerte dont il peut assurer la direction. Il sensibilise et informe les utilisateurs et les administrateurs sur l'enjeu d'un tel dispositif.

- Mettre en œuvre une chaîne d'alerte.

L'ARSSI met ou fait mettre en place un dispositif rapide et réactif qui lui permet d'alerter les différents acteurs d'un système d'information. Ce dispositif est modulable selon la criticité de l'alerte. Il s'assure que

des exercices réguliers permettent d'en vérifier l'efficacité. En cas d'alerte, il informe sa hiérarchie et les responsables concernés, fait valider les premières mesures et en demande leur application. Il s'assure de leur mise en œuvre.

- Traiter les incidents.

L'ARSSI s'assure que les acteurs du système d'information sont informés des bons réflexes en cas d'incident et que des dispositifs sont mis en place pour garantir la continuité ou la reprise d'activité dans des conditions de sécurité acceptées par les responsables concernés. Des mécanismes sont mis en place pour contenir l'incident. Il prévient les autorités compétentes et contacte le CERT concerné.

- Sauvegarder et faire analyser les journaux.

L'ARSSI s'assure que les journaux sont analysés selon une périodicité adaptée aux ressources disponibles. Il garantit leur archivage et leur intégrité.

- Glossaire –

Système d'information

L'ensemble des moyens humains et matériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire des données.

Système informatique

Ensemble de moyens informatique et de télécommunication ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire des données

SMSI

Système de management de la sécurité de l'information. Défini par la norme ISO 270001.

IGC

Infrastructure de gestion des clés.

CERT

Computer Emergency Response Team. Entité qui centralise les demandes d'assistance, traite les alertes et réagit aux attaques informatiques, qui diffuse des avis faisant état des vulnérabilités et des moyens de s'en prémunir.