



DIRECTION INTERMINISTÉRIELLE DU NUMÉRIQUE
ET DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION DE L'ÉTAT



RESEAU INTERMINISTÉRIEL DE L'ÉTAT

POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION

[RI.013]

Version 2.0 – juin 2019

Fiche de contrôle du document**Caractéristiques du document**

Identification :	NP-RI03-PSSI_RIE-v2.0
Objet :	Politique de Sécurité du Système d'Information
Version :	Version 2.0 du 14/06/2019

Contributeurs

NOM Prénom (trigramme)	Fonction
SAUNIER Guillaume (GSA)	RSSI du SCN RIE
PERREAU Franck (FPE)	RSSI Adjoint du SCN RIE
MARICHEZ Raphael (RMA)	Chef du SCN RIE

Suivi des versions

Version	Date	Rédacteur	Relecteur	Modification
2RC0.1	29/08/2018	GSA		Rédaction de la version initiale du document
2RC0.2	29/10/2018	FPE	GSA	Réalignement du plan du document à celui de la PSSI-E Réalignement du fond au service existant Prise en compte de la vision cible
2RC0.3	08/02/2019	FPE	GSA	Intégration du CoSec dans ORG.11 Lien avec la PSSI-SPM pour la bureautique
2RC0.4	01/04/2019	GSA	FPE	Ajout conditions de sortie du RIE
2RC0.5	02/05/2019	GSA	FPE	Mise en cohérence avec l'analyse de risque Finalisation
2.0	14/06/2019	Pôle SSI		Validation et mise en application

Processus de validation

Émetteur/Rédacteur	Approbateur
Nom : Pôle SSI du SCN RIE Date : 07/05/2019	Nom : Chef du SCN RIE Date : 14/06/2019

Liste de diffusion

Société / Service	Nom	Objet de la diffusion
DINSIC / SCN RIE		
ANSSI		
GT SSI		

Sommaire

Partie 1	Cadre d'emploi	5
	Avant-propos	6
1.1	Objet et champ d'application de la PSSI-RIE.....	6
1.1.1	Périmètre d'application de la PSSI	6
1.1.2	Définition, rôles et responsabilités des acteurs	7
1.2	Entrée en vigueur.....	8
1.3	Pilotage et évolutions de la PSSI-RIE.....	8
1.4	Suivi et contrôle de l'application de la PSSI	8
Partie 2	Enjeux et Objectifs.....	10
2.1	Enjeux en matière de sécurité pour le RIE.....	11
2.2	Objectifs de sécurité identifiés pour le RIE.....	11
2.3	Objectifs de la PSSI.....	13
Partie 3	Règles de sécurité.....	14
3.1	Organisation de la sécurité	15
3.2	Raccordement au RIE.....	15
3.3	Accords conclus avec des tiers.....	16
3.4	Gestion des biens.....	17
3.4.1	Responsabilités relatives aux biens.....	17
3.4.2	Protection des informations.....	17
3.4.3	Ressources humaines	18
3.5	Sécurité physique et environnementale.....	19
3.5.1	Catégorisation et zonage.....	20
3.5.2	Contrôle des accès physiques.....	21
3.5.3	Protection du matériel	22
3.5.4	Services généraux.....	22
3.5.5	Sélection et maintenance du matériel	23
3.5.6	Sécurité des matériels hors des locaux	23
3.5.7	Mise au rebut, recyclage de matériels	24
3.6	Gestion de l'exploitation.....	24
3.6.1	Procédures et responsabilités liées à l'exploitation.....	24
3.6.2	Résistance aux défaillances.....	25
3.6.3	Administration et supervision	25
3.6.4	Gestion de la prestation de service par un tiers	26
3.6.5	Interconnexion de réseaux.....	27
3.6.6	Gestion des flux et du routage	27
3.6.7	Gestion des journaux.....	28
3.7	Contrôle des accès logiques.....	28

3.8	Acquisition, développement et maintenance des systèmes d'information	29
3.8.1	Sécurité des développements et logiciels	30
3.8.2	Sécurité des configurations	30
3.8.3	Gestions des éléments secrets	30
3.9	Gestion des incidents	31
3.10	Gestion du plan de continuité et de reprise de l'activité	32
3.11	Conformité aux règles et mesures de sécurité	32
Partie 4	Annexes	35
4.1	ANNEXE I – Zones de sécurité	36
4.1.1	Zones de sécurité par typologie de matériel	36
4.1.2	Zones de sécurité par typologie de sites	37
4.2	ANNEXE II – Exemples de sensibilité des biens informationnels	40
4.2.1	Distinction entre « sensible » et « diffusion restreinte » :	40
4.2.2	Biens informationnels de diffusion restreinte	40
4.2.3	Biens informationnels classifiés de défense	40
4.3	ANNEXE III – Métriques	42
4.3.1	Échelles de besoins de sécurité et des attendus de service rendu	42
4.3.2	Échelle de disponibilité	42
4.3.3	Échelles de vraisemblance	46
4.3.4	Matrice de criticité des risques et critère de traitement	47

Table des illustrations

Figure 1 – Périmètre physique du RIE	7
Figure 2 – Echelle de disponibilité	42
Figure 3 – Échelle d'intégrité	43
Figure 4 – Échelle de confidentialité	44
Figure 5 – Échelle de traçabilité	44
Figure 6 – Échelle de gravité	45
Figure 7 – Échelle de vraisemblance	46
Figure 8 – Matrice de criticité des risques	47

Partie 1 Cadre d'emploi

Avant-propos

Le RIE dispose d'un *glossaire des sigles et dictionnaire des termes* référencé **[RI.015]** ainsi que d'un *corpus documentaire de référence*, unifié et normalisé, référencé **[RI.016]**. Les références entre crochet **[REF]** figurant dans le présent document renvoient à ce corpus documentaire.

Sauf mention contraire, ce document ainsi que les documents de référence qui y sont recensés sont librement consultables et peuvent être obtenus sur simple demande auprès du RSSI du RIE.

1.1 Objet et champ d'application de la PSSI-RIE

Le SCN-RIE, service à compétence nationale, est soumis aux dispositions générales de la politique de sécurité des systèmes d'information de l'État (PSSI-E). Etant soutenu, pour ce qui relève de la bureautique courante, par les services du Premier ministre (SPM) il est également assujéti au respect des règles de la *politique de sécurité des systèmes d'informations des services du Premier ministre* **[RRS.02]** pour ce qui concerne ce seul périmètre. La présente PSSI fixe les principes, règles et conditions de mise en œuvre composant la *politique de sécurité des systèmes d'information du RIE* **[RI.013]**.

La PSSI-RIE s'applique à tout l'écosystème du système d'information du RIE mis en œuvre par le SCN-RIE, ce dernier étant décrit en détail dans le document *Ecosystème du RIE* **[RI.011]**.

Elle doit être observée et mise en œuvre par l'ensemble des personnes physiques ou morales intervenant dans ce SI, qu'il s'agisse des administrations de l'État et de leurs agents ou bien de tiers (partenaires, prestataires ou sous-traitants) et de leurs employés.

Dans le cadre de l'utilisation du système d'information du RIE mis en œuvre par le SCN-RIE par les bénéficiaires, il est entendu que les règles imposées par leur propre PSSI devront être cohérentes (donc au minimum au même niveau) que les règles édictées par la PSSI-RIE.

Dans le cas des systèmes aptes à traiter des informations classifiées de défense, soumis à un corpus réglementaire spécifique, qui utiliseraient le RIE en tant que vecteur de transport, il appartient aux responsables des acteurs concernés d'assurer une cohérence entre l'application des dispositions de la présente PSSI-RIE et la réglementation relative à la protection des informations classifiées de défense.

1.1.1 Périmètre d'application de la PSSI

La présente PSSI s'applique à toutes les ressources matérielles, logicielles ou humaines, propres au SCN RIE ou appartenant aux différents acteurs, qui :

- permettent de rendre les services fournis par le RIE ou y contribuent,
- permettent d'exploiter le RIE ou contribuent à son exploitation,
- manipulent des informations relatives au RIE, notamment d'exploitation, ou issues du SCN RIE.

La présente PSSI doit être diffusée à l'ensemble des personnes concernées ou devant ou souhaitant être informées de son contenu et de ses éventuelles évolutions.

L'illustration ci-dessous précise le périmètre physique du RIE sur lequel s'applique la présente PSSI.

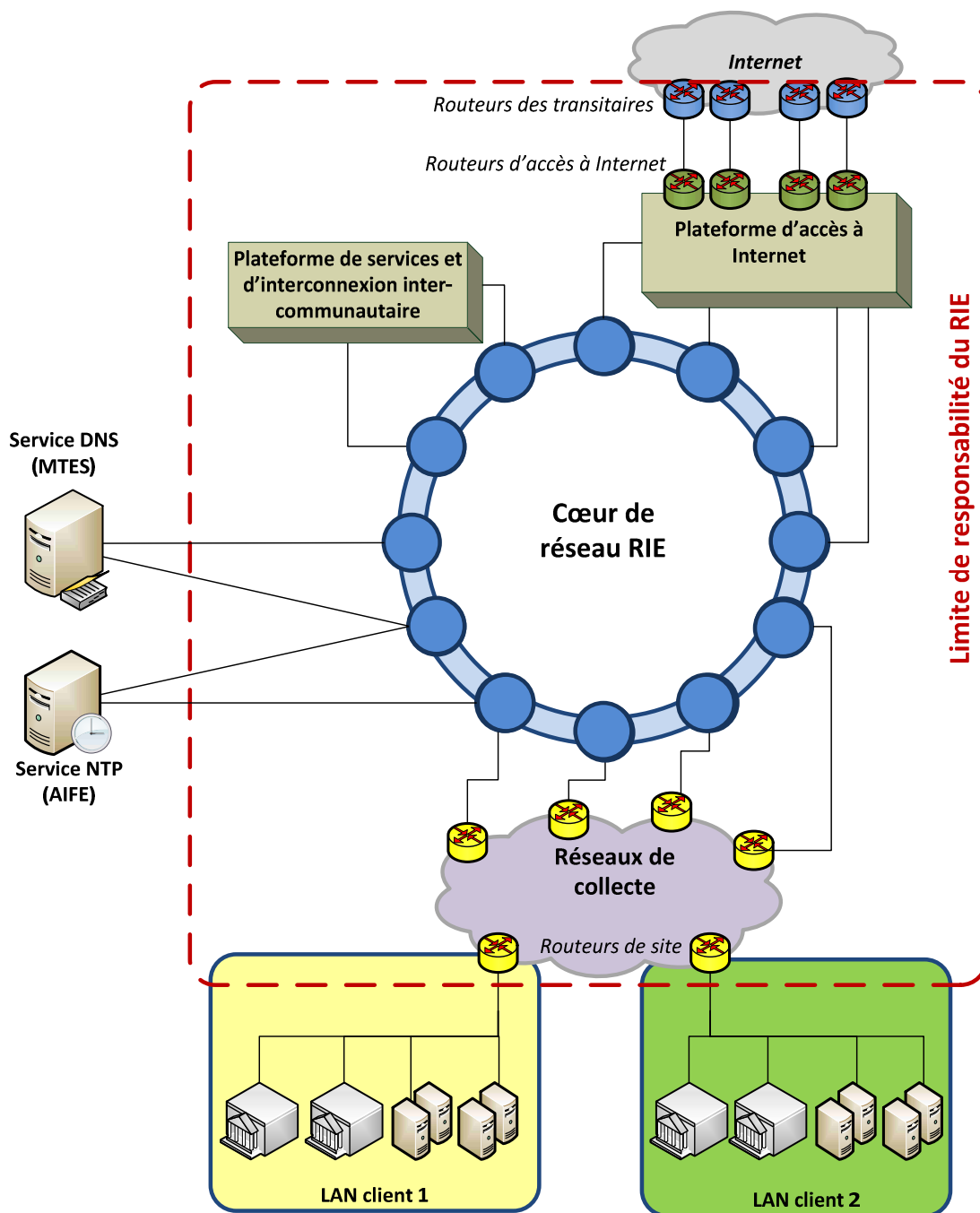


Figure 1 – Périmètre physique du RIE

1.1.2 Définition, rôles et responsabilités des acteurs

Le rôle et les missions des acteurs intervenant dans l'écosystème du SI RIE sont précisément définis dans le *Référentiel des acteurs* [RI.012]

En complément, l'organisation mise en place en matière de sécurité des systèmes d'information pour couvrir les objectifs de sécurité identifiés pour le RIE sont formalisés et détaillés dans la *note organisationnelle en matière de SSI* [RI-014].

La formalisation de cette organisation est indispensable pour que chaque acteur puisse mettre en œuvre ses responsabilités face aux enjeux de sécurité.

L'ensemble des acteurs est tenu d'appliquer et faire appliquer la présente PSSI sur son périmètre de responsabilité.

1.2 Entrée en vigueur

La PSSI-RIE entre en vigueur le jour de sa publication.

Les bénéficiaires et partenaires raccordés au RIE avant la date de publication de la présente PSSI-RIE disposent d'un délai maximum de 6 mois à compter de la publication pour mettre à jour leurs déclarations de conformité visant l'application des règles nouvellement introduites ou mises à jour.

La mise en conformité des bénéficiaires et partenaires raccordés au RIE après la date de publication fait partie intégrante du processus de raccordement. Dans ce cas, le délai pour l'application des règles de la présente PSSI-RIE ne saurait excéder 12 mois.

La mise en conformité des prestataires et fournisseurs avec les règles nouvellement introduites ou mises à jour par la présente PSSI-RIE sera intégrée au pilotage de chacun des marchés concernés dans un délai maximum de 6 mois à compter de la publication.

Dans l'éventualité de difficultés de mise en conformité, un comité de suivi pourra être mis en place avec le SCN RIE, dont le but sera notamment :

- Identifier les écarts majeurs entre les PSSI du bénéficiaire concerné et du SCN RIE ;
- Arbitrer les choix d'alignement considérés en tenant compte des impacts sur les activités ainsi que des moyens financiers et humains à mettre en œuvre ;
- Etablir un calendrier de mise en conformité indiquant les mesures à prendre dans l'immédiat puis à court et à long terme ;
- Assurer le suivi du plan d'actions co-construit.

La présente PSSI-RIE doit être diffusée par le RSSI du RIE à l'ensemble des personnes concernées devant ou souhaitant être informées de son contenu et de ses éventuelles évolutions.

1.3 Pilotage et évolutions de la PSSI-RIE

La PSSI-RIE est amenée à évoluer dans le temps. Elle pourra notamment être revue afin de prendre en compte :

- les évolutions des menaces et les retours d'expérience des traitements d'incidents ;
- les résultats d'analyses de risques ainsi que les actions découlant de contrôles ou d'inspections ;
- les évolutions des contextes organisationnel, juridique, réglementaire et technologique.

Conformément à la *Stratégie d'homologation [RI.031]*, toute révision de l'analyse de risques ou de l'état de la menace, conduite par le RSSI du RIE à son initiative ou sur décision de l'autorité d'homologation, entraîne automatiquement la révision de la présente PSSI. À cette fin, le RSSI du RIE anime les groupes de travail SSI de consultation puis de validation, sous responsabilité du chef du SCN RIE.

1.4 Suivi et contrôle de l'application de la PSSI

Le RSSI du RIE est garant de la bonne application de la présente PSSI sur l'ensemble du périmètre considéré, en s'appuyant sur les FSSI ministériels pour leurs périmètres de responsabilité respectifs. En cas de non-respect de la présente PSSI, le RSSI du RIE peut prendre, ou faire prendre, en

concertation avec les tiers concernés, toute mesure visant à garantir la sécurité de l'ensemble du réseau.

Les FSSI ministériels contrôlent et garantissent la bonne application de la présente PSSI-RIE sur le périmètre dont ils ont la charge. Ils contrôlent et garantissent également la bonne application de la présente PSSI-RIE sur les partenaires pour lesquels le ministère a demandé ou validé le raccordement. Le RSSI du RIE, sur son initiative ou sur demande du GT SSI, peut demander aux FSSI concernés de justifier de la bonne application de la présente PSSI-RIE.

Les chaînes fonctionnelles SSI des bénéficiaires sont en charge d'appliquer ou de faire appliquer la présente PSSI-RIE sur les périmètres dont elles ont la charge par tous les moyens techniques ou humains à leur disposition.

Partie 2 Enjeux et Objectifs

2.1 Enjeux en matière de sécurité pour le RIE

Le Conseil des ministres du 25 mai 2011 a décidé la mise en place d'un « réseau interministériel sécurisé regroupant l'ensemble des réseaux des ministères et permettant la continuité de l'action gouvernementale en cas de dysfonctionnement grave d'Internet ».

À ce titre le Service à Compétence Nationale « Réseau Interministériel de l'État », créé par voie d'arrêté au 17 décembre 2012 **[RRS.01]**, se substitue à l'ensemble des réseaux de transport ministériels, hors réseaux spécifiques ou classifiés, permettant la continuité de l'action gouvernementale et la conduite des politiques publiques.

De par sa fonction centrale, les enjeux en matière de sécurité pour le RIE portent à la fois sur la protection des infrastructures et informations permettant au SCN RIE de rendre et garantir le service qu'il délivre, mais également sur sa contribution à la protection des systèmes d'information et des informations de l'État.

Des analyses de risques successives ont mis en évidence qu'un incident sur le RIE pouvait avoir des conséquences importantes pour l'État, comme :

- l'impossibilité de mettre en œuvre une politique publique ou de délivrer un service public critique pouvant ainsi conduire à l'aggravation des crises majeures (sanitaires, sociales, financières, etc.),
- l'atteinte à l'image et à la crédibilité de l'action de l'État, notamment vis-à-vis des citoyens, en empêchant la délivrance de services publics attendus par ceux-ci (sécurité, versement de prestation,...),

Par ailleurs, le RIE doit contribuer à l'amélioration continue de la sécurité globale face à un accroissement des risques et des attaques pouvant peser sur les systèmes d'information de l'État :

- en permettant une meilleure coordination dans la prévention, la protection, la détection et la réaction face aux attaques,
- en réduisant la surface d'attaque potentielle de chacun des réseaux des bénéficiaires.

Cet enjeu nécessite une bonne maîtrise du RIE, des niveaux de sécurité souhaités et des risques résiduels qui empêcheraient la réalisation des objectifs de sécurité attendus sous peine d'exposer l'ensemble des systèmes d'information de l'État.

Le processus d'analyse de risques doit être régulièrement réexaminé afin de s'assurer de l'adéquation des mesures face aux évolutions continues des risques et des menaces.

2.2 Objectifs de sécurité identifiés pour le RIE

Les principaux objectifs de sécurité pour les services rendus par le RIE, ainsi que les impacts en cas de non-respect de ces objectifs sont résumés ci-après.

La fonction principale du RIE est de fournir un service de transport des flux de niveaux 2 (Ethernet) et 3 (IP), permettant l'acheminement de ces flux dans le cadre du périmètre de responsabilité du SCN RIE. Le SCN RIE doit garantir :

- un fonctionnement du transport des flux sans indisponibilité supérieure à deux heures sur les sites critiques sous peine de conduire à l'impossibilité d'assurer des services critiques pour l'État,
- la maîtrise du routage des flux et un cloisonnement logique de ceux-ci entre communautés sous peine de conduire à la diffusion d'information à des destinataires non légitimes, accroître les risques d'incidents de sécurité (virus, vers, etc.) ou leur propagation.

Le RIE propose également l'interconnexion physique et logique du RIE avec les réseaux tiers des partenaires. Concernant ce service, le SCN RIE doit garantir :

- un fonctionnement de ces interconnexions sans indisponibilité supérieure à deux heures afin que les ministères puissent échanger avec des partenaires vitaux,
- la maîtrise des échanges de flux entre le RIE et les réseaux tiers auxquels il est connecté. L'échange de flux non autorisés peut induire une diffusion d'information à des destinataires non légitimes et exposer les systèmes d'informations des bénéficiaires et partenaires à des incidents de sécurité (virus, vers, etc.).

En complément, le RIE assure la sécurité du RIE vis-à-vis d'Internet et fournit aux différents bénéficiaires une interconnexion physique et logique de leurs réseaux avec Internet. Dans ce cadre, le SCN RIE doit garantir :

- un fonctionnement de ce service sans indisponibilité supérieure à une heure. L'absence d'échange avec Internet peut conduire à l'impossibilité pour les ministères de communiquer avec l'extérieur et ainsi porter atteinte à l'action de l'État ou empêcher la diffusion d'informations critiques auprès des citoyens,
- la parfaite maîtrise des échanges de flux avec Internet sous peine d'un accroissement de l'exposition du RIE et des systèmes d'information ministériels aux attaques en provenance d'Internet ou de la divulgation non souhaitée d'informations vers Internet.

Afin de permettre les échanges interministériels, le SCN RIE doit garantir un fonctionnement de l'accès au DNS sans indisponibilité supérieure à deux heures, l'indisponibilité de ce service pouvant empêcher les échanges interministériels. Il doit également veiller à l'intégrité des entrées de ses DNS sous peine d'empêcher les échanges entre ministères ou avec l'extérieur.

Le SCN RIE doit également garantir l'accès à la référence temporelle (NTP) mise à la disposition du domaine interministériel. Une absence de référence temporelle peut engendrer une désynchronisation d'une partie, voire de la totalité, des systèmes d'information des bénéficiaires pouvant conduire à des dysfonctionnements importants de ceux-ci, notamment en ce qui concerne les systèmes d'authentification ou de gestion des journaux d'événements.

Le RIE propose un service optionnel de chiffrement des flux de niveau 3 d'un routeur de site vers un autre routeur de site au moyen d'équipements de chiffrement dédiés, qualifiés au niveau standard par l'ANSSI. Le SCN RIE doit garantir :

- un fonctionnement des équipements de chiffrement sans indisponibilité supérieure à celle des accès réseau, à savoir deux heures pour les sites critiques. L'indisponibilité d'un équipement de chiffrement peut conduire à l'impossibilité de communiquer avec ce site,
- la confidentialité des éléments secrets des chiffreurs et l'intégrité des configurations de ceux-ci. Une compromission des éléments secrets ou d'une configuration peut entraîner la divulgation d'une partie ou de l'ensemble des informations protégées.

Le SCN RIE peut tolérer un dysfonctionnement partiel de l'administration du réseau pendant une durée maximale de quatre heures. Ce dysfonctionnement peut conduire à la mobilisation de ressources supplémentaires pour permettre la continuité du service. Le SCN RIE doit par ailleurs garantir la maîtrise de la diffusion des éléments techniques manipulés dans le cadre de l'administration et l'exploitation du réseau susceptibles de compromettre la sécurité globale du RIE et, par extension, la sécurité des systèmes d'information de l'État.

Le SCN RIE ne peut tolérer un dysfonctionnement supérieur à une heure de la supervision d'une partie importante, voire de la totalité, du réseau. Un dysfonctionnement de la supervision peut induire l'impossibilité de détecter et de traiter dans des délais rapides les incidents critiques pour le fonctionnement du réseau. Par ailleurs, le SCN RIE doit garantir la maîtrise de la diffusion et la confidentialité des informations de supervision, par exemple des incidents de sécurité, susceptibles de remettre en cause la sécurité globale du réseau et, par extension, la sécurité des systèmes d'information de l'État.

2.3 Objectifs de la PSSI

Afin de répondre aux enjeux et objectifs précédemment décrits, la présente PSSI-RIE vise à garantir la sécurité des infrastructures et informations dont dépend le fonctionnement du RIE et, par extension, la sécurité des systèmes d'information de l'État qu'il porte. Les règles formulées doivent couvrir les objectifs de sécurité identifiés pour le RIE dans l'analyse de risques, à savoir assurer :

- le maintien dans le temps du niveau de sécurité du RIE, de manière proactive ou réactive,
- la disponibilité des différents services du RIE dans le respect de ses engagements de services,
- la maîtrise des échanges d'informations et du routage des flux transportés, notamment au niveau des connexions entre communautés ou avec les réseaux tiers, afin qu'aucun flux non autorisé ne soit échangé,
- la mise en place d'un cloisonnement logique des flux entre les communautés qui le méritent et le contrôle des flux échangés entre communautés afin de détecter et de limiter la propagation d'incidents de sécurité (attaques, virus, etc.) entre communautés,
- la traçabilité des opérations réalisées sur le RIE et des flux y transitant,
- La confidentialité via chiffrement quand ce service est requis,
- l'intégrité des flux transitant sur le RIE et des différentes informations manipulées dans le cadre de son exploitation.

En cas de besoin et dans le respect des contraintes légales, le RIE doit pouvoir fournir toutes les informations nécessaires à la traçabilité des flux qu'il transporte notamment dans le cadre :

- de résolution d'incidents portant sur le RIE,
- d'assistance à la résolution d'incidents portant sur un système d'information porté par le RIE,
- de requête judiciaire.

Le SCN RIE est garant du bon acheminement et de la maîtrise des flux d'informations, dans le respect de ses engagements de services, indépendamment de leur contenu. Il incombe aux bénéficiaires et aux partenaires d'estimer le besoin de confidentialité des informations envoyées vers le réseau et de mettre en place les mesures de sécurité complémentaires qui s'avéreraient nécessaires à leur protection.

Les règles décrites dans la présente PSSI devront également permettre au RIE d'être, au moyen d'une organisation adaptée et partagée par tous ainsi que des procédures de travail ad hoc, partie prenante dans la prévention et le traitement des attaques et incidents touchant au périmètre global des systèmes d'information de l'État.

Partie 3 Règles de sécurité

3.1 Organisation de la sécurité

Les règles du présent titre visent à gérer la sécurité du RIE par la mise en place d'une organisation adaptée et partagée par tous dans laquelle les rôles et responsabilités sont identifiés, formalisés, contractualisés et compris de tous.

- ORG.01** Les différents acteurs de droit public doivent disposer d'une organisation conforme aux dispositions décrites dans la PSSI-État **[RRG.07]**. Les acteurs de droit privé doivent disposer *a minima* d'une organisation conforme aux dispositions décrites dans l'annexe 1 de l'*instruction interministérielle 901 relative à la protection des systèmes d'information sensible* **[RRG.05]**. L'organisation du RIE est décrite par la *note organisationnelle* référencée **[RI.014]**
- ORG.02** Chaque acteur est responsable de l'application de l'ensemble des règles de la présente PSSI-RIE sur son périmètre de responsabilité ainsi que par ses éventuels sous-traitants. Il informe le RSSI du RIE de toute difficulté dans l'application de ces règles.

3.2 Raccordement au RIE

- ORG.03** Tout raccordement au RIE doit se faire sur demande explicite.
- ORG.04** Tout raccordement d'un utilisateur donne lieu à la rédaction préalable d'une déclaration de conformité (cf. *note organisationnelle* **[RI.014]**) adressée au RSSI du RIE et examinée par le groupe de travail SSI.
La contractualisation se fait selon le modèle de document fournis par le SCN RIE. Ce document comprend notamment :
- les caractéristiques de gestion souhaitées pour le partenaire (VRF dédiée, disponibilité, multiples raccordements, etc.),
 - les ressources auxquelles il doit accéder,
 - la durée pour laquelle le raccordement est demandé.
- ORG.05** Le raccordement d'un partenaire doit se faire sur demande explicite adressée au SCN RIE par le bénéficiaire auquel il est rattaché. La demande de raccordement doit préciser clairement les ressources auxquelles le partenaire doit avoir accès. Le raccordement d'un partenaire déjà référencé avec un autre bénéficiaire doit donner lieu à une nouvelle demande auprès du SCN RIE.
- ORG.06** Chaque bénéficiaire doit informer dès que possible le SCN RIE de toute fin de relation avec un partenaire. Le SCN RIE procédera alors à la désactivation de l'interconnexion entre le partenaire et le bénéficiaire ministériel concerné.
- ORG.07** Le raccordement d'un partenaire au RIE n'ayant plus aucune relation avec aucun bénéficiaire doit être supprimé.
- ORG.08** Tout client ou bénéficiaire souhaitant cesser de recourir aux services du RIE doit soumettre à la validation du RSSI du RIE un plan et un calendrier de sortie dont la priorité doit être le maintien en condition de sécurité du RIE. Un comité de suivi pourra être mis en place, qui pourra être amené à arbitrer entre les différentes propositions en tenant compte des impacts sur la sécurité et les activités ainsi que des moyens financiers et humains à mettre en œuvre.
- ORG.09** Sauf exception validée par le GT-SSI sur proposition du RSSI du RIE, tout flux réseau

circulant hors du territoire national terrestre et des espaces maritimes annexés de plein droit au territoire terrestre doit faire l'objet d'un chiffrage à l'aide d'une solution validée par l'ANSSI.

Les espaces maritimes ainsi définis incluent les eaux intérieures, les eaux territoriales et les eaux archipélagiques mais excluent la zone contigüe, le plateau continental et le domaine maritime de la zone économique exclusive.

- ORG.10** Le raccordement mutualisé d'un ou plusieurs bénéficiaires sur un même site nécessite au préalable la désignation d'un responsable de site et d'un responsable de sécurité afin de fournir un contact local clairement identifié au SCN-RIE.

3.3 Accords conclus avec des tiers

- ORG.11** La totalité des prestations externalisées dans le cadre du RIE doit faire l'objet d'une contractualisation, sous forme de marché ou de convention, entre le fournisseur concerné et le SCN RIE. Cette contractualisation doit respecter les recommandations des guides publiés par l'ANSSI, en particulier et de façon non exhaustive respecter les guides suivants :

- Guide d'externalisation des systèmes d'information **[RD.01]**
- Guide d'hygiène informatique **[RD.02]**
- Note technique relative à la gestion des mots de passe **[RD.05]**
- Guide d'administration sécurisée **[RD.07]**

- ORG.12** La totalité des marchés et conventions doit inclure la capacité d'audits des équipements, mutualisés ou dédiés, y compris des systèmes d'administration et de supervision et des procédures par le SCN RIE durant toute la durée des marchés et conventions. Dans le cas d'absence de respect des mesures de sécurité demandées, les marchés prévoient les modalités de mises à niveau (responsabilité, délai, etc.) et, le cas échéant, les pénalités associées.

- ORG.13** La totalité des marchés et conventions doit inclure une clause portant obligation de confidentialité sur l'ensemble des travaux, renseignements, documents ou objets parvenus à la connaissance du fournisseur ou de l'un de ses sous-traitants dans le cadre de l'exécution des prestations délivrées. Cette obligation est valable durant toute la durée du marché ou de la convention et s'étend sur une période courant jusqu'à trois ans après la date d'achèvement.

- ORG.14** Chaque fournisseur doit s'engager à exécuter ses obligations en termes de sécurité des systèmes d'information selon un plan d'assurance sécurité (PAS) précisant les moyens mis en œuvre par celui-ci pour respecter les règles de la présente PSSI et les exigences de sécurité du RIE. Les modalités de rédaction, de révision et d'approbation de ce document contractuel sont conformes à la note organisationnelle **[RI.014]** et aux recommandations du guide d'externalisation des systèmes d'information publié par l'ANSSI **[RD.01]**. Tout titulaire d'un marché ou fournisseur pour une commande hors marché devra également participer aux instances de pilotage de la sécurité, réunies régulièrement dans le cadre de l'exécution de sa prestation, sous l'autorité du SCN RIE.

3.4 Gestion des biens

Les règles du présent paragraphe visent à assurer la connaissance et la responsabilité de chaque bien manipulé dans le cadre du RIE et de préciser les modalités de gestion afférentes.

3.4.1 Responsabilités relatives aux biens

- BIE.01** Une identification, un recensement et un étiquetage de l'ensemble des matériels utilisés dans le cadre du RIE est mis en œuvre par chaque fournisseur sur son périmètre de responsabilité. L'identification de chaque matériel sera réalisée par une référence unique sur le périmètre de chaque fournisseur concerné. À cet effet, chaque fournisseur mettra en œuvre un fichier ou une base de données centralisée dont il garantira la sauvegarde, la confidentialité et l'intégrité des données associées. Chaque fournisseur s'engage à fournir au SCN RIE, sur demande de sa part, tout ou partie des éléments de ce fichier ou de cette base de données.
- BIE.02** Chaque fournisseur doit sauvegarder et indexer l'historique complet des configurations et des versions logicielles utilisées. L'identification de chaque configuration ou version logicielle sera réalisée par une référence unique sur le périmètre de chaque fournisseur concerné. À cet effet, chaque fournisseur mettra en œuvre un fichier ou une base de données centralisée dont il garantira la sauvegarde, la confidentialité et l'intégrité des données associées. Chaque fournisseur s'engage à fournir au SCN RIE, sur demande de sa part, tout ou partie des éléments de ce fichier ou de cette base de données. En cas d'urgence, les configurations doivent être fournies au plus tôt selon une procédure d'urgence formalisée par le fournisseur et validée par le SCN RIE.
- BIE.03** Chaque fournisseur réalise des tests réguliers de restauration afin de s'assurer de la bonne sauvegarde des configurations et de sa capacité à effectuer des reprises d'activité ou des retours arrière.
- BIE.04** Toute modification d'une configuration mise en production doit faire l'objet d'un nouvel enregistrement dans la base comme nouvelle configuration de référence.

3.4.2 Protection des informations

Les informations sensibles, qu'elles soient techniques ou contractuelles doivent être protégées en confidentialité et en intégrité. Ces règles décrivent les mécanismes et procédures permettant de s'assurer que la diffusion d'informations s'effectue selon les principes du besoin d'en connaître et du moindre privilège. Elles incluent en particulier la formalisation d'une politique de catégorisation de l'information ainsi que la mise en place de contrôles d'accès logiques pour l'accès aux informations sensibles (informations techniques, éléments secrets nécessaires au chiffrement,...).

- BIE.05** Tout bien informationnel relatif au RIE, ou participant à son exploitation, doit être catégorisé suivant son besoin de confidentialité par le RSSI du RIE. L'annexe II de la présente PSSI-RIE présente des exemples des principaux types de biens informationnels considérés, les marquages et les conditions de traitement afférentes.
- BIE.06** Les biens informationnels le nécessitant doivent faire l'objet d'un marquage ou d'une mention par son émetteur en relation avec leur besoin en confidentialité.
- BIE.07** Tout bien informationnel ne faisant pas l'objet d'un marquage ou d'une mention doit faire l'objet d'une évaluation par son émetteur en relation avec son besoin en confidentialité avant transmission.

- BIE.08** Les personnes amenées à manipuler ou traiter des informations sensibles relatives au RIE doivent le faire dans le respect des procédures de gestion des informations du RIE.
- BIE.09** Le traitement des informations sensibles relatives au RIE doit utiliser, dans la mesure du possible, des produits ou des services certifiés, qualifiés ou agréés par l'ANSSI.
- BIE.10** Le traitement des informations relatives au RIE catégorisées « diffusion restreinte » doit se faire dans le respect des procédures de gestion des informations du RIE et de *l'instruction interministérielle relative aux mesures de protection des systèmes d'information traitant d'informations sensibles* non classifiées de défense de niveau Diffusion Restreinte **[RRG.05]** et notamment utiliser, dans la mesure de l'existant, des produits ou des services qualifiés par l'ANSSI.
- BIE.11** L'accès aux informations relatives au RIE, notamment par les fournisseurs, doit se faire dans le respect du besoin d'en connaître et du moindre privilège.
- BIE.12** Les lieux et conditions d'hébergement des données relatives au RIE doivent satisfaire aux exigences de sécurité du donneur d'ordres et aux dispositions de la *loi Informatique et Libertés* **[RL.01]**. En particulier, chaque fournisseur doit pouvoir communiquer au SCN RIE la liste de tous les lieux de stockage des données sur simple demande de sa part.
- BIE.13** Les informations et documents sensibles relatifs au RIE transmis par voie électronique doivent systématiquement faire l'objet d'un chiffrement adapté à leur niveau de confidentialité, validé par le RSSI du RIE.
- BIE.14** Les informations et documents sensibles relatifs au RIE stockés sur des supports transportables (smartphones, cartes mémoire, etc.) doivent faire l'objet d'un chiffrement adapté à leur niveau de confidentialité.
- BIE.15** Il incombe aux différents acteurs d'estimer le besoin de confidentialité des informations qu'ils transmettent et de mettre en place les mesures de sécurité complémentaires qui s'avéreraient nécessaires à leur protection. Pour cela, les ministères peuvent souscrire aux options de chiffrement proposées par le RIE ou mettre en œuvre sous leur responsabilité les mécanismes adaptés.
- BIE.16** Pour ce qui concerne les personnels du RIE, la transmission d'information par voie électronique ne peut être effectuée qu'à partir des seuls systèmes fournis par l'administration.

3.4.3 Ressources humaines

Ces règles ont pour but de garantir que les personnes amenées à intervenir sur le RIE sont formées, sensibilisées à la sécurité des systèmes d'information et informées de leur rôle et responsabilisées dans l'organisation mise en place pour assurer la sécurité du RIE.

- SRH.01** Le RSSI du RIE, en lien avec le FSSI des Services du Premier Ministre, s'assure que les personnels du SCN RIE sont sensibilisés à la SSI, sont informés et ont bien compris leurs rôles et responsabilités dans l'organisation mise en place pour assurer la sécurité du RIE et des services associés. Il s'assure que les procédures, notamment liées à la SSI, sont bien diffusées, comprises et appliquées par les différents personnels du SCN RIE. Le chef du SCN RIE s'assure que les personnels du RIE sont correctement formés aux tâches qui leur sont confiées.

- SRH.02** Chaque fournisseur s'assure que ses personnels sont sensibilisés à la SSI, sont correctement formés aux tâches qui leurs sont confiées, sont informés et ont bien compris leurs rôles et responsabilités dans l'organisation mise en place pour assurer la sécurité des prestations qu'ils délivrent.
- SRH.03** Chaque utilisateur s'assure que ses personnels sont sensibilisés à la SSI, sont correctement formés aux tâches qui leurs sont confiées, sont informés et ont bien compris leurs rôles et responsabilités dans l'organisation mise en place pour assurer la sécurité du RIE et des services associés.
- SRH.04** Chaque acteur s'assure que les procédures, notamment liées à la SSI, sont bien diffusées, comprises et appliquées par ses différents personnels.
- SRH.05** Chaque acteur informe ses personnels, par tous moyens à sa convenance, sur leurs obligations de confidentialité, par exemple par contrat ou signature par son personnel intervenant sur le RIE d'une charte de confidentialité. Ces obligations de confidentialité sont applicables à tous les personnels, y compris après leur départ.
- SRH.06** Chaque acteur met en place les sanctions adaptées pour toute personne ayant contrevenu aux règles de sécurité de la présente PSSI-RIE.
- SRH.07** Chaque acteur met en place les procédures adaptées pour que la restitution de tout matériel et la suppression de tout droit d'accès soient effectuées au départ d'un de ses personnels.
- SRH.08** Les personnels exploitant les équipements de chiffrement traitant des informations de niveau « diffusion restreinte » configurés ou en production, notamment ayant accès aux éléments secrets, doivent être habilités à traiter des informations de niveau « Confidentiel Défense ».

3.5 Sécurité physique et environnementale

Ces règles visent à restreindre l'accès physique aux équipements du RIE et à formaliser les procédures d'accès : personnels autorisés, méthodes utilisées pour le contrôle physique (contrôle supplémentaire pour l'accès en salle du PIB), habilitation des agents... Elles précisent également les conditions dans lesquelles les équipements du RIE doivent être hébergés et stockés. Ces règles décrivent enfin les modalités d'intervention sur les sites hébergeant des équipements du RIE (PIB, sites bénéficiaire sensibles,...).

3.5.1 Catégorisation et zonage

PHY.01 Catégorisation de sites. Les sites hébergeant des ressources nécessaires au fonctionnement du RIE sont répartis entre les trois catégories suivantes :

- **Catégorie A** - Un site de catégorie A héberge des services critiques pour le SCN RIE. Son indisponibilité peut avoir un impact maximum sur les services qu'il rend ou sur le fonctionnement du RIE. Cette indisponibilité ne peut pas dépasser deux heures. Les sites de catégorie A sont typiquement les PIB ou les datacenters des bénéficiaires.
- **Catégorie B** – Un site de catégorie B héberge des services sensibles pour le SCN RIE. Son indisponibilité peut avoir un impact limité à moyen sur les services qu'il rend, sans nuire à un service critique. Les sites de catégorie B sont par exemple les NR de Renater.
- **Catégorie C** - Un site de catégorie C est un site non critique pour le fonctionnement du RIE. L'indisponibilité de ce type de site a un impact limité. Les sites de catégorie C sont typiquement les points de collecte des bénéficiaires hors datacenter.

Le cas échéant, les bénéficiaires formalisent pour ce qui les concerne la catégorisation de leurs sites selon les mêmes critères, en fonction de l'impact d'une indisponibilité. Ils communiquent la catégorisation retenue afin de vérifier l'adéquation des moyens de raccordement au RIE.

PHY.02 Zonage. Tout local hébergeant des ressources informatiques du RIE doit pouvoir être classé dans une des quatre typologies suivantes :

- **Zone rouge** : zone garantissant une protection à l'état de l'art en matière de contrôle des accès physiques et des conditions d'hébergement du matériel : détection/extinction automatique des incendies, locaux hors d'eau, alimentation électrique secourue, doublement des arrivées télécommunication et fluides suivant des arrivées distinctes, contrôles d'accès nominatifs, détection d'intrusion, etc.
- **Zone orange** : zone garantissant un niveau de sécurité renforcé en matière de protection des accès physique. Elle est équipée de dispositifs de détection d'intrusion et de contrôle nominatif des accès, en plus des dispositifs déjà présents sur une zone verte.
- **Zone verte** : zone ne nécessitant pas de mesures autres que les mesures de base en matière de protection physique telles que le contrôle d'accès, la présence d'extincteur ou de systèmes de détection d'incendie. Cette zone correspond au niveau de sécurité par défaut des locaux ne contenant pas de ressources ou de données sensibles.
- **Zone non classée** : ce sont des zones pour lesquelles le niveau de sécurité n'est pas contrôlé ou maîtrisé. Elles doivent donc être considérées comme des zones « non maîtrisées » dans le cadre du fonctionnement du RIE. Ce sont typiquement des zones d'accueil (hall, entrée) ou des aires de livraison.

Le tableau ci-après résume les mesures de protection requises pour chaque type de zone.

Catégorie de mesures	Zone Rouge	Zone Orange	Zone Verte	Zone Non classée
Hébergement / protection contre les sinistres	Détection/ extinction automatique des incendies Locaux hors d'eau, hors zone inondable Alimentation électrique secourue Doublement des arrivées télécom Doublement des dispositifs de climatisation	Détection incendie	Détection incendie	Non connu
Contrôle d'accès	Contrôle d'accès physique nominatif	Contrôle d'accès physique nominatif	Contrôle d'accès physique	Non connu
Détection des intrusions	Détection des intrusions avec levée de doute immédiate	Détection des intrusions avec levée de doute immédiate ou a posteriori	Optionnel	Non connu

Tab. 1 – Mesures applicables par type de zone

PHY.03 Tout équipement en propre au RIE (routeur de cœur de réseau, routeur de site, plateforme de services) ou traitant des informations relatives au RIE (contrats, documentation techniques, journaux d'évènements) doit être situé dans une zone correspondant à son niveau de criticité. La liste des zones applicables en fonction de chaque type de matériel est précisée en annexe I.

PHY.04 Un responsable de la sécurité physique doit être nommément désigné pour toute zone rouge ou orange ainsi que pour tout site mutualisé. Par défaut, l'officier de sécurité du site concerné sera désigné et chargé de la mise en œuvre et du contrôle des moyens de protection mis en place.

3.5.2 Contrôle des accès physiques

PHY.05 Les différentes zones sont délimitées et protégées par des périmètres de sécurité (murs, portes avec contrôle d'accès le cas échéant).

PHY.06 Une politique de restriction des accès physiques doit être définie et appliquée pour les différentes zones limitant l'accès aux seules personnes ayant le besoin d'y pénétrer.

PHY.07 Une procédure d'autorisation est mise en place pour les différentes zones. Cette procédure inclut une liste nominative des personnes autorisées à pénétrer dans les zones hébergeant les équipements du SCN RIE et à intervenir sur les équipements informatiques (techniciens, fournisseurs). La liste des autorisations d'accès est gérée et maîtrisée par le responsable de la sécurité physique de la zone avec les informations fournies par le SCN RIE. Cette gestion ne peut être déléguée à un prestataire tiers. Le responsable de la sécurité physique de la zone et le RSSI du RIE sont chacun

responsables de la mise à jour de la liste nominative des intervenants autorisés pour leur périmètre de responsabilité et informe l'autre partie des mises à jour.

- PHY.08** Pour les sites de catégorie A et B, les interventions doivent se faire dans le cadre d'une procédure formalisée. Elle indique *a minima* les personnes à contacter lors d'une intervention, les modalités et facilités d'accès aux sites et aux équipements en condition nominale ou particulière (heures non ouvrables, crise, etc.) ainsi que toute information de nature à simplifier l'intervention (plan des locaux, plan des salles, etc.).
- PHY.09** L'accès des visiteurs aux différentes zones fait l'objet d'un contrôle d'accès, avec traçabilité et conservation des motifs de l'intervention et un accompagnement systématique par le personnel autorisé du site. Cette traçabilité des accès est auditable, *a minima* pendant un an.
- PHY.10** Les zones vertes sont protégées par des contrôles d'accès permettant de s'assurer que seul le personnel autorisé peut y pénétrer.
- PHY.11** Les zones rouges et orange doivent disposer d'un contrôle nominatif des accès (par exemple système de badge nominatif) avec traçabilité des entrées. Le système de contrôle des accès doit être *a minima* conforme aux recommandations du *guide sur les contrôles d'accès* publié par l'ANSSI [RD.03]
- PHY.12** Pour chaque site, *a minima* un binôme de correspondants locaux sera identifié comme contact à prévenir pour les interventions.

3.5.3 Protection du matériel

- PHY.13** Dans les zones rouges, les équipements du RIE sont hébergés dans des baies (pour les équipements en exploitation) ou des armoires (pour les équipements de secours) dédiées et fermées à clé. Une procédure de gestion des clés est mise en place pour permettre l'accès aux équipements en heures ouvrées comme en heures non ouvrées. Le responsable de la sécurité physique de la zone est en charge de définir et faire appliquer cette procédure.
- PHY.14** Une procédure d'acheminement sécurisé des équipements de chiffrement, configurés ou pré-personnalisés, sur les sites de bénéficiaires doit être formalisée par le fournisseur et validée par le SCN RIE.
- PHY.15** Les équipements de secours préconfigurés doivent être stockés dans des conditions identiques à celles prévues pour le matériel de production.

3.5.4 Services généraux

- PHY.16** Les équipements du RIE hébergés dans des zones rouges sont situés dans un local prévu à cet effet, dans des conditions d'hébergement adaptées, correctement dimensionnés et secourus (alimentation électrique, climatisation, détection incendie avec extinction automatique, etc.).
- PHY.17** L'alimentation électrique des équipements hébergés dans des zones rouges doit être assurée en continue et être redondée. L'utilisation d'un onduleur permettant d'assurer la continuité de l'alimentation électrique en cas de panne est recommandée. En cas de panne prolongée, l'alimentation électrique doit être assurée par un générateur de

secours de type groupe électrogène.

- PHY.18** L'alimentation en fluides des zones rouges doit être redondée et suffisante pour assurer l'alimentation des systèmes de climatisation ou d'extinction des incendies. Par ailleurs des extincteurs manuels doivent être stockés dans la zone en cas de dysfonctionnement du système d'extinction d'incendie.
- PHY.19** Les servitudes techniques, assurant ces conditions d'hébergement, doivent faire l'objet d'une maintenance régulière dont les comptes-rendus sont auditables et stockés pendant une durée minimale de 3 ans.

3.5.5 Sélection et maintenance du matériel

- MAT.01** L'ensemble des services fournis par le RIE doit l'être au moyen de matériels dédiés au RIE. Conformément aux recommandations du *guide d'externalisation des systèmes d'information* publié par l'ANSSI **[RD.01]**, toute solution d'hébergement mutualisé est proscrite sans accord explicite du SCN RIE.
- MAT.02** Tous les matériels utilisés doivent être maintenus en conditions opérationnelles et de sécurité soit par le SCN RIE en propre, soit par le fournisseur ou un prestataire accrédité par le constructeur du matériel. Le propriétaire du matériel doit gérer son obsolescence. Si l'exploitation est assurée par un prestataire mais que ce dernier n'est pas propriétaire du matériel, il ne peut néanmoins déroger à son devoir de conseil envers le SCN RIE en restant force de proposition quant à la construction d'un planning de remplacement dudit matériel.
- MAT.03** Les équipements pour lesquels des failles de sécurité ou des piégeages sont avérés doivent faire l'objet d'une procédure adaptée pouvant aller jusqu'à la proscription du matériel.
- MAT.04** Les équipements de chiffrement traitant de l'information de niveau « Diffusion Restreinte » doivent être qualifiés au niveau standard par l'ANSSI.
- MAT.05** Les équipements de raccordement des sites bénéficiaires ou partenaires au RIE sont ceux disponibles au titre des marchés du RIE.
- MAT.06** Les équipements du RIE ne doivent pas mettre en œuvre de technologies sans fil, qu'elles soient de nature hertzienne ou autre, sauf dérogation validée par le RSSI du RIE.
Il en va de même pour les équipements déployés à la demande des bénéficiaires, les dérogations étant du ressort des FSSI concernés.

3.5.6 Sécurité des matériels hors des locaux

- MAT.07** Pour chaque type de matériel, des procédures de livraison, de remplacement, d'effacement sécurisé, de retour en usine et de reconditionnement doivent être formalisées par chaque fournisseur et validées par le SCN RIE.
- MAT.08** Les matériels livrés doivent être systématiquement testés et vérifiés par les fournisseurs du RIE à réception. Tout échec des tests menés donne lieu à un retour en usine du matériel et à la notification du SCN RIE.
- MAT.09** Les équipements stockés hors des sites de production (dans des locaux titulaires

notamment) ne doivent pas être transportés avec leur configuration opérationnelle.

3.5.7 Mise au rebut, recyclage de matériels

- MAT.10** Les engagements de remplacement des matériels défectueux ou non-conformes doivent être formalisés et contractualisés avec les différents fournisseurs.
- MAT.11** Une procédure d'effacement sécurisé lors de la mise au rebut, la fin de vie ou le reconditionnement des matériels doit être formalisée par le RSSI du RIE. Cette procédure doit préciser les moyens mis en œuvre pour assurer l'effacement effectif des données. Selon la criticité du matériel considéré, ils pourront aller de la réécriture simple des disques à la destruction physique des supports de stockage. Cette règle est applicable à tout matériel utilisé dans le cadre du RIE et recensé.
- MAT.12** La fin de vie des éléments secrets ou des équipements de chiffrement donne lieu à la destruction physique ou logique des supports permettant de les stocker conformément à l'*instruction interministérielle 910 relative aux articles contrôlés de la SSI [RRG.06]*.
- MAT.13** En cas de fin de vie, de remplacement, de mise au rebut ou de compromission d'un équipement de chiffrement, un service de dépersonnalisation, activable en local ou à distance doit être mis en œuvre. Cette dépersonnalisation assure un effacement complet des éléments secrets. Elle peut être déclenchée sur demande du FSSI du bénéficiaire impacté ou du RSSI du RIE.

3.6 Gestion de l'exploitation

Ces règles présentent les conditions dans lesquelles le RIE doit être exploité et supervisé afin d'en assurer la sécurité.

3.6.1 Procédures et responsabilités liées à l'exploitation

Ces règles formalisent les modalités de mise à jour des équipements ou les opérations de maintenance sur les équipements du RIE.

- EXP.01** Le SCN RIE est responsable de la supervision de la totalité du RIE. Il met en place des moyens techniques et organisationnels adaptés à ses missions conformément à la *note organisationnelle [RI.014]*.
- EXP.02** Chaque fournisseur est responsable de l'administration et de la supervision du périmètre dont il a la charge. Il met en place des moyens techniques et organisationnels adaptés, conformément à la *note organisationnelle [RI.014]*.
- EXP.03** Avant toute mise en production, l'ensemble des procédures d'exploitation et de supervision pour chaque type d'équipement doit être formalisé par le fournisseur, validé par le SCN RIE et diffusé auprès des personnels exploitant. Ces procédures doivent inclure *a minima* :
- un test préalable sur un équipement représentatif et indépendant de l'équipement en exploitation,
 - l'utilisation des seules mises à jour fournies et approuvées par le fabricant,
 - la réalisation de tests de non régression,
 - la capacité de retour arrière dans des délais contraints quelle que soit l'évolution mise en œuvre en suivant des procédures formalisées par les fournisseurs exploitant les équipements et validées par le SCN RIE,

- la fourniture systématique d'un rapport de test, puis d'un rapport de mise en production au SCN RIE,
- la validation par le SCN RIE de toute action avant déploiement en production.

- EXP.04** Tout intervenant est tenu de respecter les procédures d'exploitation et de supervision en vigueur.
- EXP.05** Avant toute mise en production, le service doit faire l'objet d'une recette fonctionnelle sur la base d'un cahier de test validé. Seul le SCN RIE est habilité à prononcer la conformité de la recette.
- EXP.06** Toute intervention sur un équipement, en particulier susceptible de porter atteinte aux objectifs de sécurité du RIE, doit être signalée au SCN RIE.
- EXP.07** La programmation des opérations de maintenance et de mises à jour est réalisée de préférence en HNO avec l'accord explicite du SCN RIE et du bénéficiaire impacté.
- EXP.08** Des tests réguliers de restauration doivent être réalisés afin de s'assurer de la bonne sauvegarde des configurations et de la capacité de chaque fournisseur à effectuer des reprises d'activité ou des retours arrière.
- EXP.09** Les fournisseurs en charge de l'exploitation des équipements doivent appliquer systématiquement les patches de sécurité des constructeurs, *a minima* sur les services activés.

3.6.2 Résistance aux défaillances

Ces règles ont pour but d'optimiser le fonctionnement du réseau pour détecter au plus vite les défaillances et ainsi assurer les engagements de services.

- DEF.01** L'architecture globale du RIE, les protocoles utilisés et la configuration des équipements doivent garantir le fonctionnement du réseau en cas de défaillance d'un équipement ou d'un lien. L'architecture adoptée ne doit pas faire apparaître de points uniques de défaillance non explicitement identifiés et acceptés par le RSSI du RIE.
- DEF.02** Les sites de catégorie A (cf. §3.5.1) doivent être doublement raccordés au RIE avec le niveau de sécurisation adaptée. Le choix des modalités de raccordement (technologie et opérateur) est du ressort du bénéficiaire responsable du site.

3.6.3 Administration et supervision

Ces règles décrivent l'ensemble des mesures à mettre en place pour assurer une gestion optimale des flux d'exploitation des équipements du RIE. Ces mesures visent à garantir la protection, notamment en intégrité et confidentialité des données de supervision, utilisées notamment par le NOC/SOC et les fournisseurs.

- ADM.01** Les flux d'administration des équipements du RIE doivent transiter sur un réseau logique différent de ceux utilisés pour les flux de données et protégés en confidentialité et en intégrité vis-à-vis d'Internet.
- ADM.02** Les données de supervision du RIE doivent transiter sur un réseau logique différent de ceux utilisés pour les autres flux de données et protégés en confidentialité et intégrité

- ADM.03** Chaque fournisseur, bénéficiaire ou partenaire assure le maintien en conditions opérationnelles et de sécurité des systèmes d'information connectés au RIE qu'il met en œuvre, en particulier ceux servant à l'administration et à la supervision. À ce titre, il met en œuvre les recommandations du *guide d'hygiène informatique* de l'ANSSI [RD.02].
- ADM.04** L'administration et la supervision des équipements du RIE doivent se faire à l'aide de matériels dédiés à cet usage, fournis et maîtrisés par le fournisseur ou ses éventuels sous-traitants. L'administration et la supervision des équipements du RIE avec du matériel personnel ou non maîtrisé sont proscrites.
- ADM.05** L'usage de matériels nomades ou de terminaux mobiles pour l'administration et la supervision des équipements du RIE est autorisé uniquement pour du matériel professionnel à l'état de l'art après validation du RSSI du RIE.
- ADM.06** Les personnels exploitant doivent, en cas de fin de contrat, restituer tout équipement leur ayant été remis dans le cadre de leurs fonctions.
- ADM.07** La connexion de support amovibles aux équipements du RIE et au système d'administration et de supervision doit être limitée au strict nécessaire et faire l'objet d'une autorisation formelle du responsable de la sécurité concerné.
- ADM.08** Tout support amovible doit être analysé, *a minima* au moyen d'un antivirus, avant connexion aux équipements du RIE et aux systèmes d'administration et de supervision.
- ADM.09** L'exécution des « autorun » sur les supports amovibles doit être désactivée.
- ADM.10** La connexion de tout périphérique personnel (PDA, téléphone, ordinateur personnel, carte mémoire, clé USB, etc.) aux équipements du RIE et aux systèmes d'administration et de supervision est interdite, même aux seules fins de recharge électrique.

3.6.4 Gestion de la prestation de service par un tiers

Ces règles visent à garantir les engagements et la qualité du service rendu par le RIE et notamment à éviter tout risque d'engorgement du réseau pouvant induire des indisponibilités.

- SLA.01** Une mesure continue des engagements de services (SLA) doit être mise en place par chaque fournisseur sur les prestations qui lui incombent.
- SLA.02** Une évaluation continue sur l'utilisation des liens et la capacité de traitement des équipements est mise en place par chaque fournisseur et le SCN RIE.
- SLA.03** L'estimation de la capacité de traitement des équipements doit systématiquement prendre en compte la charge supplémentaire induite par une défaillance.
- SLA.04** Une politique de gestion d'évolution du réseau doit être formalisée. Elle indique notamment les règles d'évolution des liens ou plateformes de services en fonction de leur utilisation.
- SLA.05** La qualité des FON doit être contrôlée, *a minima* tous les 3 ans (avec tests poussés de

3.6.5 Interconnexion de réseaux

Ces règles ont pour but de s'assurer que les ouvertures de flux avec les réseaux tiers externes au RIE sont maîtrisées. Les échanges avec les réseaux tiers ne peuvent se faire que par des plateformes d'interconnexion et de protection dédiées, notamment la plateforme d'accès à Internet (PFAI).

- RSX.01** Les équipements de cœur de réseau du RIE ne doivent pas être exposés sur Internet.
- RSX.02** Toute interconnexion d'un système d'information connecté au RIE avec un réseau tiers, y compris celui d'un partenaire national ou international, doit faire l'objet d'une homologation. Cette homologation doit être portée à la connaissance du RIE et figurer dans la déclaration de conformité du bénéficiaire concerné.
- RSX.03** Tous les échanges de flux en provenance et à destination d'Internet doivent être contrôlés au moyen de sondes de sécurité.
Les échanges de flux IP en provenance et à destination d'Internet doivent transiter par la Plate-Forme d'Accès à Internet (PFAI) du RIE.
Tout flux dérogatoire doit être filtré par des plateformes de protection homologuées, sous le contrôle du FSSI du bénéficiaire concerné, et porté à la connaissance du RSSI du RIE.

3.6.6 Gestion des flux et du routage

Ces règles ont pour but de s'assurer que les ouvertures de flux entre les différentes communautés du RIE sont maîtrisées.

- FLX.01** Toute interconnexion entre communautés doit être réalisée par le SCN RIE au moyen des plateformes de filtrage mises en œuvre au niveau du cœur de réseau.
Tous les échanges de flux entre communautés doivent être contrôlés au moyen de sondes de sécurité
- FLX.02** Par défaut, les flux entre communautés sont fermés sur les configurations en production. Un suivi régulier de la part du SCN RIE doit être mis en place afin de vérifier la pertinence des flux ouverts entre communautés.
- FLX.03** Les règles de routage intracommunautaires seront implémentées conjointement par le SCN RIE et le bénéficiaire concerné, selon les besoins exprimés par le bénéficiaire en prenant en compte les contraintes techniques et organisationnels du RIE.
- FLX.04** Un partenaire ne pourra échanger qu'avec le ou les bénéficiaires pour lequel le raccordement a été demandé et uniquement pour les ressources demandées.
- FLX.05** Les réseaux des partenaires sont raccordés au RIE sur des communautés spécifiques (VRF) à ces partenaires. Les partenaires ayant un grand nombre de sites raccordés au RIE peuvent disposer d'une communauté dédiée après validation du SCN RIE.
- FLX.06** L'hébergement sur un même matériel de services mutualisés entre communautés doit garantir le cloisonnement des flux et informations entre chaque communauté. En particulier, toute technique de virtualisation doit garantir l'étanchéité des flux et informations de chaque compartiment virtuel et fournir les moyens de contrôles

- FLX.07** Toute remontée automatique d'informations vers les constructeurs de matériel doit faire l'objet d'une autorisation explicite du RSSI du RIE et doit être désactivée par défaut quand cela est possible.

3.6.7 Gestion des journaux

Ces règles décrivent les modalités de gestion et de protection des journaux issus de l'exploitation du RIE.

- JOU.01** La gestion et la sauvegarde des journaux doit se faire selon les modalités fixées par la politique de gestion des journaux. Cette politique précise en particulier, pour chaque fournisseur et pour le SCN RIE :
- les durées de conservation pour chaque type de journaux,
 - les moyens de conservation mis en œuvre selon la sensibilité des journaux,
 - les modalités de mise à disposition, éventuellement via une procédure d'urgence, des journaux du RIE au SCN RIE sur simple demande (pour les journaux conservés chez les fournisseurs),
 - les modalités d'indexation des journaux sauvegardés pour en faciliter l'exploitation,
 - les modalités de modification du niveau de précision des journaux.
- JOU.02** Les systèmes de journalisation et de stockage des journaux d'événement doivent disposer de mécanismes assurant l'intégrité et la confidentialité des journaux.
- JOU.03** L'accès logique aux journaux est restreint aux seules personnes ayant le besoin d'en connaître selon le principe du moindre privilège.
- JOU.04** Chaque bénéficiaire et fournisseur a uniquement accès aux journaux relatifs à son périmètre de responsabilité. Le SCN RIE et l'ANSSI peuvent avoir accès à l'ensemble des journaux.
- JOU.05** La durée de rétention des journaux est d'un an pour l'ensemble des services du RIE.
- JOU.06** Le niveau de précision des journaux collectés doit pouvoir être modifiable rapidement afin :
- de limiter la production de journaux aux éléments strictement nécessaires en fonctionnement nominal,
 - de pouvoir augmenter le niveau de précision en cas de besoin notamment en cas de suspicion d'incident de sécurité ou de demande de l'autorité légitime.
- JOU.07** Les journaux d'événements des équipements de chiffrement ou des services de sécurité associés doivent être fournis sur simple demande du SCN RIE ou du bénéficiaire ministériel.

3.7 Contrôle des accès logiques

- ACC.01** L'accès logique aux équipements utilisés dans le cadre du RIE doit être protégé par des mécanismes d'authentification et limité aux seules personnes autorisées.
- ACC.02** Une procédure de gestion des accès logiques aux équipements et à l'information doit

être formalisée afin d'empêcher les accès non autorisés. Cette procédure précise que :

- toute demande d'accès logique doit être formalisée par le demandeur et soumise à validation de la personne en charge des équipements ou de l'information concernée,
- les demandes d'accès et les validations résultantes sont auditable pendant une durée minimale d'un an,
- les accès logiques effectués sur les équipements ou les consultations d'information font l'objet d'une journalisation,
- l'ensemble des actions d'administration sont journalisées, nominatives et horodatées. Selon les capacités des équipements, les opérations d'administration seront enregistrées afin qu'elles puissent être rejouées au besoin,
- lors d'un départ ou d'une cessation d'activité d'un personnel, tous les accès logiques dont il dispose seront supprimés,
- le remplacement de personnel doit donner lieu à la mise en œuvre de comptes et d'accès propres au nouvel arrivant, distincts des accès du précédent titulaire.

ACC.03 L'authentification sur les équipements doit se faire avec l'utilisation de comptes nominatifs aux moyens de serveurs centralisés dédiés à cet effet. L'accès aux équipements doit par ailleurs être sécurisé en utilisant les mécanismes de protection adéquats.

ACC.04 Des comptes de services doivent être instanciés localement sur chaque équipement pour se prémunir du risque d'indisponibilité des serveurs d'authentification. La connaissance des éléments secrets liés à ces comptes de service doit être restreinte au seul personnel autorisé ayant le besoin d'en connaître.

ACC.05 En cas de compromission ou de divulgation, volontaire ou involontaire, d'un mot de passe, une procédure d'urgence de changement de mot de passe doit être déclenchée. Elle doit permettre le changement rapide du mot de passe tout en préservant l'accès en exploitation à l'équipement pour le fournisseur. Cette procédure doit être formalisée par le fournisseur et validée par le SCN RIE.

ACC.06 La procédure de gestion des mots de passe doit être formalisée et respecter, autant que faire se peut, les recommandations des *guides de l'ANSSI* **[RD-02]**, **[RD.05]** et **[RD.07]**. Elle inclut notamment les principes de sécurité suivants :

- changement des mots de passe lors de la première connexion,
- suppression des comptes et mots de passe génériques,
- taille minimale des mots de passe,
- durcissement des mots de passe avec emploi de majuscule, minuscule, chiffres et caractères spéciaux,
- procédure de changement du pool de mot de passe en cas d'incident de sécurité avéré le nécessitant,
- procédure d'autorisation des mots de passe de plus haut privilège.

ACC.07 Les droits d'accès de l'ensemble des exploitant doivent être supprimés dès la fin de leur période d'emploi, ou modifiés selon les modalités ad hoc en cas de modification de leur affectation.

3.8 Acquisition, développement et maintenance des systèmes d'information

3.8.1 Sécurité des développements et logiciels

- DEV.01** Chaque acteur doit assurer la sécurité et la maintenance des développements applicatifs qu'il réalise ou fait réaliser conformément à l'état de l'art dans chacune des technologies mises en œuvre.
- DEV.02** Chaque développement applicatif fait l'objet d'une recette avant mise en production comprenant une revue de code permettant de s'assurer d'une implémentation conforme aux exigences et aux bonnes pratiques de sécurité.
- DEV.03** Tous les logiciels doivent être maintenus en condition opérationnelle et de sécurité par le fournisseur, ou un prestataire accrédité par l'éditeur du logiciel. Le fournisseur doit gérer l'obsolescence du support des logiciels utilisés.

3.8.2 Sécurité des configurations

- CNF.01** Toute configuration utilisée doit pouvoir être contrôlée par le SCN RIE, en amont de la mise en production des équipements. Le SCN RIE peut demander les modifications qu'il juge nécessaire à ces configurations avant toute mise en production.
- CNF.02** Toute configuration en production doit pouvoir être contrôlée et vérifiée à tout moment par le SCN RIE.
- CNF.03** Afin d'optimiser la gestion des configurations et la cohérence du parc, il est recommandé que les configurations d'équipements délivrant des fonctions similaires soient semblables.
- CNF.04** Les services non utilisés sur les équipements sont non installés ou, lorsque cela n'est pas possible, systématiquement désactivés de manière logicielle ou physique. Toute impossibilité est signalée au RSSI du RIE.
- CNF.05** Les configurations utilisées sont limitées au strict nécessaire. En particulier, les configurations des équipements de routage se limiteront aux routes strictement nécessaires.
- CNF.06** Les options de sécurité additionnelles proposées par les constructeurs sont systématiquement étudiées et peuvent être rendues obligatoires après examen par le SCN RIE.
- CNF.07** Dans la mesure du possible, les configurations doivent être communes à l'ensemble des communautés afin d'en simplifier la gestion, la maintenance et de minimiser le risque d'erreur.

3.8.3 Gestions des éléments secrets

Le terme « éléments secrets » désigne ici les clés secrètes des chiffreurs matériels utilisés dans le cadre du RIE ainsi que les informations permettant l'administration de ces clés.

- CNF.08** Les équipements de chiffrement doivent faire l'objet d'une procédure d'exploitation spécifique incluant les moyens mis en œuvre pour la gestion et l'exploitation des éléments secrets.
- CNF.09** Les procédures d'exploitation des équipements de chiffrement doivent assurer la

confidentialité et l'intégrité des éléments secrets utilisés selon les modalités imposées par les règles du §3.4.2 (Protection des informations) de la présente PSSI-RIE.

- CNF.10** La génération, l'affectation et l'introduction des éléments secrets dans les équipements de chiffrement doivent se faire lors d'une opération formalisée garantissant à tout moment la confidentialité et l'intégrité des éléments secrets. Cette opération doit se dérouler en présence de l'opérateur chargé du chiffre ou du représentant du FSSI du bénéficiaire considéré. Tout manquement à cette procédure nécessite la destruction des secrets générés et la reprise de l'opération.
- CNF.11** Tout au long du cycle d'utilisation de l'équipement de chiffrement, la protection en confidentialité et en intégrité des éléments secrets doit être assurée. L'accès aux éléments secrets doit s'effectuer uniquement au moyen d'une authentification forte.
- CNF.12** L'accès aux éléments secrets est limité à une liste restreinte de personnes nommément identifiées. Ces personnes doivent disposer d'une habilitation à manipuler des informations classifiées au sens de *l'instruction générale interministérielle 1300 [RRG.08]* au niveau immédiatement supérieur à celui des éléments secrets considérés.
La liste de ces personnes est maintenue par le RSSI ou le responsable du chiffre du bénéficiaire utilisant l'équipement de chiffrement. Une copie de cette liste peut être fournie au RSSI du RIE, sur demande de celui-ci.
- CNF.13** Une procédure de révocation des éléments secrets ou des certificats d'administration permettant l'accès à ces éléments secrets doit être mise en place. Le FSSI du bénéficiaire considéré ou le RSSI du RIE peuvent déclencher cette procédure en cas de compromission des éléments secrets.

3.9 Gestion des incidents

Cette partie décrit les mesures et procédures à appliquer pour gérer au mieux les incidents de sécurité rencontrés lors de l'exploitation du RIE, de leur détection proactive jusqu'à leur résolution.

Un incident de sécurité désigne un ou plusieurs événements compromettant ou susceptibles de compromettre la sécurité des services fournis par le RIE, les informations nécessaires à son exploitation et, par extension, l'activité et la sécurité des systèmes d'information de ses bénéficiaires.

Ces règles décrivent les outils et services mis en place afin de lutter de manière proactive contre les incidents de sécurité, incluant les attaques contre le RIE ou les systèmes d'information qu'il porte. Elles ont pour objectif de minimiser la gravité des impacts que ces incidents pourraient avoir sur le RIE.

- INC.01** Chaque acteur met en place une organisation adaptée permettant le traitement des incidents. Il applique les procédures de gestion des incidents, approuvées par le SCN RIE, conformément à la *note organisationnelle [RI.014]*.
Les procédures de gestion des incidents doivent inclure les modalités d'escalade et de gestion de crise en cas d'incident majeur le nécessitant.
- INC.02** L'ensemble des demandes et des incidents relatifs au RIE fait l'objet d'un enregistrement sous responsabilité du SCN RIE dans un outil de gestion des tickets.
Le SCN RIE assume également la responsabilité de classifier l'incident et son niveau d'impact, de traiter l'incident avec les parties concernées et de le clôturer avec la

confirmation de la résolution par le déclarant.

- INC.03** L'ensemble des demandes et des incidents relatifs au RIE fait l'objet d'une revue régulière afin de s'assurer de leur traitement et de leur clôture effective.
- INC.04** Le SOC du RIE assure une veille de sécurité afin d'identifier les éventuelles menaces et vulnérabilités portant sur le périmètre global du RIE.
- INC.05** Chaque fournisseur assure une veille de sécurité afin d'identifier les éventuelles menaces et vulnérabilités portant sur les prestations qu'il délivre.
- INC.06** Chaque fournisseur informe le SCN RIE dès identification d'un incident, d'une potentielle menace ou de vulnérabilités sur le périmètre dont il a la charge.
Il en analyse les causes et l'impact potentiel ou atteint.
Il propose les mesures correctives appropriées.
Pour les vulnérabilités avérées, le fournisseur concerné propose un correctif testé et l'applique selon les modalités de mises à jour des équipements (cf.§3.6.1 3.6.1-*procédures et responsabilités liées à l'exploitation*).
- INC.07** Chaque bénéficiaire ou partenaire informe le SCN RIE dès identification d'un incident de sécurité sur son périmètre susceptible de porter atteinte aux objectifs de sécurité du RIE et indique les mesures correctives qu'il envisage de mettre en œuvre.

3.10 Gestion du plan de continuité et de reprise de l'activité

Ces règles décrivent les mesures relatives à la continuité de l'activité du RIE et à sa reprise, en cas de sinistre majeur.

- PCA.01** Chaque fournisseur formalise et maintient un plan de reprise et de continuité d'activité sur son périmètre de responsabilité. Il soumet ce plan pour validation au chef du SCN RIE, sur avis du RSSI du RIE.
- PCA.02** Le plan de reprise d'activité doit permettre, en cas de sinistre, d'assurer les services les plus critiques du RIE selon les objectifs de sécurité identifiés par l'analyse de risques.
- PCA.03** Le SCN RIE coordonne au niveau global du RIE un plan de reprise d'activité s'appuyant sur ceux définis par les différents fournisseurs, dont il vérifie la cohérence.
- PCA.04** Le SCN RIE s'assure, notamment au moyen de tests réguliers, que tous les fournisseurs sont en mesure d'appliquer les PCA/PRA. Les plans de reprise ou de continuité d'activité sont activés en cas de besoin sur décision du chef du SCN RIE ou du fournisseur, après information et validation du chef du SCN RIE.
- PCA.05** Les plans de reprise et de continuité d'activité mis en œuvre par les bénéficiaires ou partenaires doivent être mis en cohérence avec les principes techniques et organisationnels du RIE.
- PCA.06** Les dispositions permettant d'assurer le PCA/PRA doivent être révisées régulièrement, *a minima* annuellement.

3.11 Conformité aux règles et mesures de sécurité

Ces règles visent à vérifier le respect des règles et mesures de sécurité par des contrôles réguliers sur les équipements, les configurations et les procédures en vigueur, notamment chez les différents fournisseurs.

- REG.01** Des contrôles réguliers du niveau de sécurité et de l'efficacité des mesures de protection mises en œuvre doivent être réalisés par les équipes en charge de l'exploitation sur chaque périmètre de responsabilité considéré. Ces contrôles doivent permettre de mettre en évidence le plus rapidement possible les anomalies et incidents et conduire à la mise en œuvre des mesures correctrices appropriées.
- REG.02** Toute anomalie d'utilisation ou écart par rapport aux mesures de protection doit faire l'objet d'un rapport et d'un plan de mise en œuvre des mesures correctrices appropriées transmis au RSSI du RIE.
- REG.03** Des contrôles et des audits, à périodicité adaptée aux risques et aux enjeux, doivent être réalisés afin de vérifier la conformité avec les règles de la présente PSSI-RIE. Conformément à la norme ISO 27002, cet exercice doit permettre une appréciation des possibilités d'amélioration et une approche de gestion de la sécurité de l'information compte tenu des changements intervenant dans l'environnement organisationnel, des circonstances liées à l'activité, des conditions légales ou de l'environnement technique. Un plan de contrôle et d'audit sera ainsi formalisé chaque année par le RSSI du RIE. Il planifiera les actions de contrôle et d'audit en fonction des priorités fixées par le groupe de travail SSI. Ce plan de contrôle n'exclut pas la réalisation d'audits non planifiés, qui peuvent être décidés à l'initiative du RSSI du RIE ou de l'autorité d'homologation.
- REG.04** Un contrôle de sécurité sera systématiquement effectué après tout incident de sécurité (cf. §3.9 – *gestion des incidents*3.9) mettant en lumière des manquements dans l'application et le respect des règles de sécurité de la présente PSSI-RIE.
- REG.05** Un contrôle de sécurité doit être réalisé, préalablement à la mise en production ou à la modification du périmètre physique ou fonctionnel de chaque service du RIE. Ce contrôle doit permettre de vérifier la conformité du service dans son ensemble à la PSSI-RIE et aux règles de sécurité.
- REG.06** Le SCN RIE et le bénéficiaire exploitant l'équipement de chiffrement ont la capacité d'auditer, sur simple demande, la politique de sécurité déployée sur les équipements de chiffrement de son périmètre ou les services de sécurité associés.
- REG.07** Tout audit de sécurité fera systématiquement l'objet d'un compte rendu, pouvant être assorti de mesures correctives à appliquer et d'un calendrier de mise en conformité. Un audit de vérification pourra être effectué pour vérifier cette mise en conformité.
- REG.08** Les rapports d'audit porteront *a minima* les mentions « diffusion restreinte » en raison des failles de sécurité sur le RIE ou son exploitation pouvant apparaître dans ceux-ci. En fonction des failles de sécurité mises en évidence dans le rapport, celui-ci pourra être classifié « Confidentiel Défense » et/ou porter la mention « Spécial France » sur décision du RSSI du RIE.
- REG.09** L'accès aux outils de contrôle et d'audit doit être restreint et maîtrisé.
- REG.10** Les contrôles ne doivent pas perturber le fonctionnement nominal du RIE ou du SI

considéré de manière imprévue.

REG.11 Des indicateurs mesurables de contrôle doivent être définis par le groupe de travail SSI et mis en œuvre pour vérifier le respect des règles de sécurité de la présente PSSI-RIE. Ces indicateurs sont consolidés dans des tableaux de bord par le RSSI du RIE qui les présente *a minima* annuellement à la commission d'homologation.

Partie 4 Annexes

4.1 ANNEXE I – Zones de sécurité

4.1.1 Zones de sécurité par typologie de matériel

Matériel	Typologie de zone de sécurité
Matériel des PIB	Zone rouge
Matériels des sites bénéficiaires	Zone rouge , orange ou verte en fonction de la catégorie du site.
Équipement de chiffrement	Zone rouge ou orange en fonction de la catégorie du site.
Matériel stocké chez les titulaires sans configuration hors équipement de chiffrement	Zone non classée
Matériel stocké avec configuration minimale hors équipement de chiffrement	Zone verte
Matériel stocké avec une configuration opérationnelle hors équipement de chiffrement	Zone identique à celle du matériel considéré en production
Matériel d'administration et de supervision du RIE	Serveurs en zone rouge et postes en zone orange
Matériel d'administration et de supervision des titulaires	Serveurs en zone rouge et postes en zone orange

4.1.2 Zones de sécurité par typologie de sites

4.1.2.1 Sites de catégorie A

Un site de catégorie A héberge des services critiques pour le bénéficiaire ou le SCN RIE. Son indisponibilité peut avoir un impact maximum sur le fonctionnement du bénéficiaire, les services qu'il rend ou sur le fonctionnement du RIE. Cette indisponibilité ne peut pas dépasser deux heures. Les sites de catégorie A sont typiquement les PIB ou les datacenters des bénéficiaires.

Type de raccordement proposé		CoS	GTR proposé	Secours proposés	Zone associée
FO	de 100Mbps à 10Gbps	5 classes des données : - 1 classe voix/temps réel - 1 classe vidéo - 2 classes données - 1 classe "best effort"	N4 : < 1 heure 24h/24 7j/7 N3 : < 2 heures 24h/24 7j/7	G : Double lien fibre optique avec double cheminement/adduction et double rattachement (2 PoP) et double pénétration site bénéficiaire F : Double lien fibre optique avec double cheminement/adduction et double rattachement (2 PoP) E : Double lien fibre optique avec double cheminement/adduction	Rouge
FO	de 100Mbps à 500Mbps		N4 : < 1 heure 24h/24 7j/7 N3 : < 2 heures 24h/24 7j/7	A : Lien simple sans sécurisation	Rouge

4.1.2.2 Sites de catégorie B

Un site de catégorie B héberge des services sensibles pour le bénéficiaire ou le SCN RIE. Son indisponibilité peut avoir un impact limité à moyen sur le fonctionnement du bénéficiaire ou des services qu'il rend, sans nuire à un service critique. Les sites de catégorie B sont typiquement des sites bénéficiaires rassemblant un personnel important et permettant de rendre des services importants (préfecture,...).

Type de raccordement proposé		CoS	GTR proposé	Secours proposés	Zone associée
FO	de 6Mbps à 10Gbps	5 classes des données : - Une classe voix/temps réel - Une classe vidéo - Deux classes données - Une classe "best effort"	N2 : < 4 heures 24h/24 7j/7 N1 : < 4 heures 8h-19h du lundi au vendredi	G : Double lien fibre optique avec double cheminement/adduction et double rattachement (2 PoP) et double pénétration site bénéficiaire F : Double lien fibre optique avec double cheminement/adduction et double rattachement (2 PoP) E : Double lien fibre optique avec double cheminement/adduction	Orange
FO	de 4Mbps à 20Mbps		N2 : < 4 heures 24h/24 7j/7 N1 : < 4 heures sur la plage 8h-19h du lundi au vendredi	D : Lien fibre optique et lien de secours SDSL	Orange
SDSL	de 512Kbps à 8Mbps (selon éligibilité)		N2 : < 4 heures 24h/24 7j/7 N1 : < 4 heures sur la plage 8h-19h du lundi au vendredi	C : Double lien SDSL avec rattachement à 2 DSLAM B : Double lien SDSL ou SDSL secouru avec un lien ADSL ou 3G	Orange

4.1.2.3 Sites de catégorie C

Un site de catégorie C est un site non critique pour le fonctionnement du bénéficiaire ou des services qu'il rend. L'indisponibilité de ce type de site a un impact limité pour le bénéficiaire. Les sites bénéficiaires d'importance moindre rentrent dans cette catégorie.

Type de raccordement proposé		CoS	GTR proposé	Secours proposés	Zone associée
FO	de 4Mbps à 500Mbps	5 classes des données : - Une classe voix/temps réel - Une classe vidéo - Deux classes données - Une classe "best effort"	N2 : < 4 heures 24h/24 7j/7 N1 : < 4 heures sur la plage 8h-19h du lundi au vendredi	A : Lien simple sans sécurisation	Verte
SDSL	de 512Kbps à 8Mbps (selon éligibilité)		N2 : < 4 heures 24h/24 7j/7 N1 : < 4 heures sur la plage 8h-19h du lundi au vendredi	A : Lien simple sans sécurisation	Verte
ADSL	de 8Mbps à 20Mbps (selon éligibilité)	Une classe « best effort »	N/A	A : Lien simple sans sécurisation	Verte

4.2 ANNEXE II – Exemples de sensibilité des biens informationnels

Cette annexe présente quelques exemples de biens informationnels associés à leurs niveaux de sensibilité théorique.

4.2.1 Distinction entre « sensible » et « diffusion restreinte » :

La frontière entre les marquages « sensible » et « diffusion restreinte » est ténue et ne repose sur aucun fondement juridique. Il est généralement admis que la diffusion d'une donnée « sensible » doit être limitée et que si cette limitation est restreinte à un groupe de personnes, à une communauté ou à un domaine de confiance identifiés alors elle doit être marquée « diffusion restreinte ».

Entrent par exemple dans la catégorie des biens informationnels susceptibles d'être considérés comme « sensibles » jusqu'à « diffusion restreinte » les biens suivants, pour autant qu'ils ne fassent pas par ailleurs l'objet d'un marquage ou d'une classification spécifique :

- Les documents contractuels
- Les procédures d'exploitation
- Les documents techniques ne présentant pas d'éléments vitaux ni la totalité du réseau et ne permettant pas de reconstituer ces informations

4.2.2 Biens informationnels de diffusion restreinte

Les informations « diffusion restreinte » sont celles dont la diffusion doit être maîtrisée et restreinte à un groupe de personnes, à une communauté ou à un domaine de confiance voire aux seules personnes ayant besoin de la connaître dans l'exercice de leurs attributions.

Le traitement des biens informationnels de diffusion restreinte se fait dans le respect des *instructions interministérielles 901 [RRG.05]* en ce qui concerne les systèmes d'informations de données sensibles et *910 [RRG.06]* pour les articles contrôlés de sécurité des systèmes d'information.

Entrent par exemple dans la catégorie des biens informationnels de diffusion restreinte :

- Les documents techniques présentant des éléments vitaux ou la totalité du réseau et les documents permettant de reconstituer ces informations
- Les documents préparatoires à la publication de marchés publics
- Les plans de continuité d'activité et de reprise d'activité après sinistre ne faisant pas l'objet d'une classification de défense
- Les informations liées à la gestion de la sécurité et ne faisant pas l'objet d'une classification de défense
- Les rapports d'audits ne faisant pas l'objet d'une classification de défense
- Les éléments secrets des équipements de chiffrement de niveau « DR » ne permettant pas le déchiffrement par eux-mêmes.

4.2.3 Biens informationnels classifiés de défense

Les informations classifiées de défense sont définies et régies par l'*instruction générale interministérielle 1300 [RRG.08]*.

Entrent par exemple dans la catégorie des biens informationnels classifiés de défense :

- Certaines informations liées à la gestion de la sécurité et notamment au traitement des failles et incidents
- Les rapports d'audits faisant apparaître des failles de sécurité.

4.3 ANNEXE III – Métriques

4.3.1 Échelles de besoins de sécurité et des attendus de service rendu

Afin d'exprimer les besoins de sécurité des biens essentiels du SCN RIE, quatre critères de sécurité sont retenus : la disponibilité, l'intégrité, la confidentialité et la traçabilité. D'une manière générale, on les désigne par l'expression « critères DICT ».

Les besoins de sécurité, étudiés lors de l'analyse de risque, portent sur les principes mis en œuvre par le SCN-RIE pour rendre les services attendus par les utilisateurs du RIE. Ces attendus de services rendus s'expriment également selon les critères DICT.

4.3.2 Échelle de disponibilité

L'échelle de **disponibilité** est proposée sous forme d'une double échelle permettant d'évaluer d'un côté les besoins en disponibilité des biens essentiels du RIE et de l'autre les attendus de services rendus par les utilisateurs, répartis selon quatre axes en fonction :

- de la GTR en heures ouvrées ;
- de la GTR en heures non ouvrées ;
- du temps d'indisponibilité maximale cumulée sur 12 mois glissants ;
- du nombre d'occurrence d'un incident causant une perte de disponibilité.

Les besoins et attendus en **disponibilité** sont évalués en fonction des niveaux suivants :

ECHELLE DE DISPONIBILITE					
	BESOINS	ATTENDUS			
		GTR-HO	GTR-HNO	TIMC sur 12 mois glissants	Occurrences
4	la durée d'indisponibilité doit rester d'au maximum une heure	Inférieure à 1h	Inférieure à 1h	Inférieur à 2h	Inférieur à 3 occurrences
3	une durée d'indisponibilité d'au plus 4 heures mais supérieure à 1h est acceptable	Inférieure à 2h	Inférieure à 2h	Inférieur à 4h	Inférieur à 5 occurrences
2	une durée d'indisponibilité d'au plus 24 heures mais supérieure à 4h est acceptable	Inférieure à 4h	Inférieure à 4h	Inférieur à 12h	Inférieur à 10 occurrences
1	une durée d'indisponibilité supérieure à 24h est acceptable	Supérieure à 4h	Supérieure à 4h	Inférieur à 24h	Supérieur à 10 occurrences

Figure 2 – Echelle de disponibilité

4.3.2.1 Échelle d'intégrité

L'échelle d'**intégrité** est proposée sous la forme de deux échelles permettant d'évaluer ce critère de sécurité selon que l'on considère :

- l'intégrité propre à l'information portée par le bien essentiel comme par exemple l'intégrité d'un flux de données ;
- l'intégrité du service rendu : celui-ci est-il conforme à ce qui est attendu du service ?

Les besoins et attendus en **intégrité** sont évalués selon les niveaux :

ECHELLE D'INTEGRITE		
	Échelle applicable à une information	Échelle applicable à un service
4	Doit être rigoureusement intègre, aucune altération n'est acceptable. L'intégrité doit pouvoir être vérifiée.	Les engagements de services et les procédures permettant de rendre ce service doivent être formalisés. Les procédures et engagements doivent être scrupuleusement respectés.
3	Doit être intègre. L'absence d'intégrité doit pouvoir être détectée automatiquement le plus rapidement possible et être réparable. L'intégrité doit pouvoir être vérifiée.	Les engagements de services sont formalisés et doivent être respectés. Des procédures d'exécution peuvent être formalisées et mises en place.
2	Peut ne pas être intègre, mais l'altération doit pouvoir être détectée. L'intégrité doit pouvoir être vérifiée.	Les engagements de services sont formalisés. L'absence de respect des engagements de service sur une courte période peut être tolérée.
1	Une perte ou modification non prévue, volontaire ou non volontaire, n'affecte en rien les activités d'un service.	Aucun besoin d'engagement de service ou de formalisation des processus d'exécution.

Figure 3 – Échelle d'intégrité

4.3.2.2 Échelle de confidentialité

L'échelle de **confidentialité** est proposée sous la forme de deux échelles permettant d'évaluer ce critère de sécurité selon que l'on considère :

- La confidentialité propre à une information;
- La confidentialité du service rendu

Les besoins et attendus en **confidentialité** sont évalués en fonction des niveaux suivants :

ECHELLE DE CONFIDENTIALITE		
	Échelle applicable à une information	Échelle applicable à un service
4	L'information bénéficie d'une protection métier, d'un marquage « diffusion restreinte » ou est soumise à une réglementation impliquant une protection particulière	Aucun échange de flux, entre communautés ou domaines de confiance différents, ne doit être fait par le service. La diffusion de l'information doit être restreinte aux seules personnes ayant besoin de la connaître dans l'exercice de leurs attributions.
3	L'information est sensible et ne doit être accessible qu'à des personnes identifiées	L'échange de flux, entre communautés ou domaines de confiance différents, doit être explicitement autorisé et faire l'objet de mécanismes de contrôle. La diffusion de l'information doit être maîtrisée et restreinte à un groupe de personnes, à une communauté ou à un domaine de confiance.
2	L'information est à usage interne, réservée ou l'administration ou à des partenaires identifiés	L'échange de flux, entre communautés ou domaines de confiance différents, doit être maîtrisé. La diffusion de l'information doit être limitée, cependant une divulgation fortuite mais limitée de l'information peut être tolérée.
1	L'information est publique ou pourrait être diffusée sans conséquence	Les flux n'ont aucun besoin de cloisonnement et peuvent être échangés librement entre communautés ou domaines de confiance différents. La divulgation d'information, même en masse, est autorisée car celle-ci est soit publique ou soit déjà protégée par des moyens d'offuscation.

Figure 4 – Échelle de confidentialité

4.3.2.3 Échelle de traçabilité

L'échelle de **traçabilité** prend en compte à la fois le besoin sur la production de traces, opposables ou non, et le besoin en termes de durée de conservation de ces traces.

Les besoins et attendus en **traçabilité** sont évalués en fonction des niveaux suivants:

ECHELLE DE TRACABILITE		
	Besoin de traces (BT)	Durée de conservation (DC)
4	Les opérations doivent être tracées de manière détaillée (qui, quoi, quand), conservées et intègres.	Supérieure à 1 an
3	Les opérations doivent être tracées de manière détaillée (qui, quoi, quand), conservées et exploitées régulièrement (statistiques, retours qualité...).	1 an
2	Les opérations doivent être tracées de manière minimale (qui, quand) et conservées pour analyse ponctuelle.	3 mois
1	Aucune traçabilité des opérations n'est requise.	1 mois

Figure 5 – Échelle de traçabilité

4.3.2.4 Échelles de gravité

La **gravité** est évaluée selon la typologie d'impact considéré avec les niveaux suivants :

ECHELLE DE GRAVITE	
4	L'événement redouté impacte l'ensemble des bénéficiaires du RIE ou empêche la mise en œuvre d'une politique publique ou la délivrance d'un service critique par un bénéficiaire. Il peut ainsi conduire à l'aggravation des crises majeures (sanitaires, sociales, financières, etc.) et porter atteinte à : ■ la sécurité globale du RIE et des systèmes d'information de ses bénéficiaires (risque de divulgation de faille de sécurité, de la topologie réseau, etc.). ■ la crédibilité de l'action de l'Etat, par exemple par des articles dans la presse. <i>Exemple : Panne du Backbone RIE empêchant le transport des flux IP sur l'ensemble de périmètre ministériels. perte du service d'interconnexion de réseau avec un partenaire lors de la gestion d'une crise sanitaire...</i>
3	L'événement redouté impacte un bénéficiaire ou une zone géographique étendue sans nuire à un service critique rendu par celui-ci. Il peut avoir un impact limité sur l'image du bénéficiaire ou du SCN RIE, par exemple par des articles dans la presse. Il est également susceptible d'engager ponctuellement et modérément la responsabilité juridique, administrative ou civile, le cas échéant pénale, du bénéficiaire ou du SCN RIE. Enfin il peut porter atteinte, de manière limitée, à la sécurité d'un service du RIE ou du système d'information d'un bénéficiaire. <i>Exemple : Perte partielle d'une plaque de collecte, diffusion involontaire d'information technique sur le cœur de réseau, etc.</i>
2	L'événement redouté impacte un site ou un nombre limité d'utilisateurs. Il peut conduire à une incapacité partielle ou totale de travail pour les utilisateurs concernés sans nuire à un service critique rendu par un bénéficiaire ou à l'image de celui-ci. Il peut nécessiter la mise en place de ressources supplémentaires par le SCN RIE ou le bénéficiaire pour assurer le service. <i>Exemple : Perte d'un lien d'un site de catégorie B, saturation d'un lien Internet d'une communauté,...</i>
1	L'événement redouté est quasiment sans impact pour le SCN RIE ou ses bénéficiaires. Il peut induire une gêne limitée à quelques utilisateurs et nécessiter une adaptation du mode de fonctionnement de travail habituel d'un bénéficiaire ou du SCN RIE. Il peut s'agir d'un événement de sécurité n'ayant pas d'impact direct et immédiat sur le bénéficiaire ou le SCN RIE. <i>Exemple : Saturation d'un lien d'un site de catégorie C, absence d'un personnel du NOC/SOC RIE...</i>

Figure 6 – Échelle de gravité

4.3.3 Échelles de vraisemblance

La **vraisemblance** est estimée suivant différents critères selon les niveaux suivants :

ECHELLE DE VRAISEMBLANCE				
	Fréquence d'apparition d'un risque récurrent.	Probabilité d'apparition d'un risque non reproductible.	Difficulté de mise en œuvre	Attractivité des ressources
4	Dans la semaine	> 80%	Ne nécessitant aucune ressource ou connaissance spécifiques	Ressources très attractives
3	Dans le mois	Entre 40 et 80%	Nécessitant des ressources et des connaissances standards	Ressources attractives
2	Dans le trimestre	Entre 5 et 40%	Nécessitant des ressources spécifiques et des connaissances avancées	Ressources peu attractives
1	Dans l'année	<5%	Nécessitant des ressources importantes et une expertise pointue	Ressources non attractives

Figure 7 – Échelle de vraisemblance

4.3.4 Matrice de criticité des risques et critère de traitement

Les scénarios de risques identifiés dans l'analyse de risques SSI sont hiérarchisés en fonction de leur gravité et de leur vraisemblance selon la matrice ci-dessous :

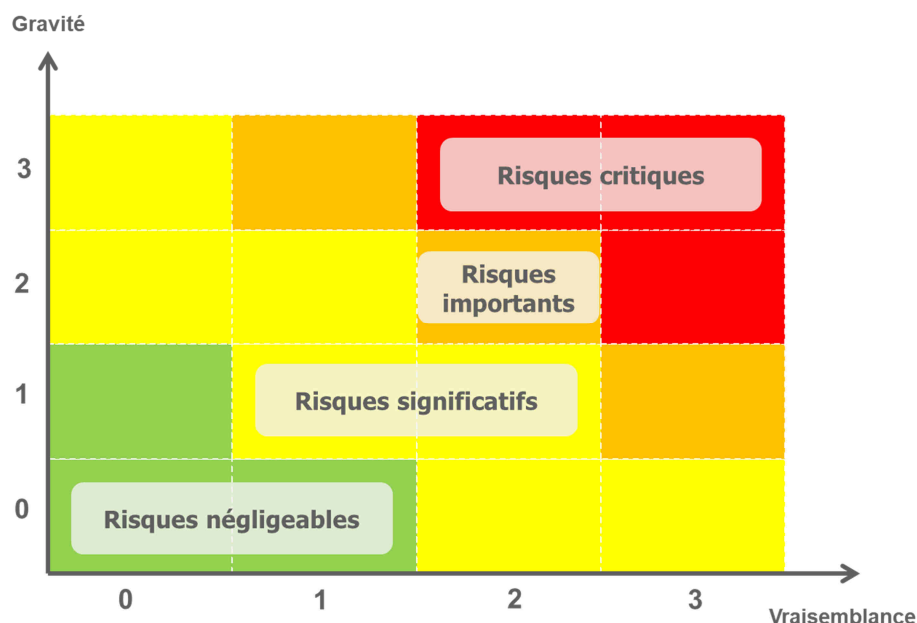


Figure 8 – Matrice de criticité des risques

Quatre niveaux de risques sont donc retenus :

- négligeable ;
- significatif ;
- important
- critique.

Les critères de traitement suivants sont retenus :

CRITICITÉ	
Niveau	Définition
NEGLIGEABLE	Le risque est, sauf exception, accepté.
SIGNIFICATIF	Le traitement du risque nécessite un arbitrage (acceptation ou traitement).
IMPORTANT	Le risque ne peut pas être accepté et doit être traité.
CRITIQUE	Le risque ne peut pas être accepté et doit être traité en priorité.