Agence Nationale de Sécurité des Systèmes d'Information | Burkina Faso

REFERENTIEL GENERAL DE SECURITE BURKINA FASO (RGS-BF)

JANVIER 2019

INFORMATIONS SUR LE DOCUMENT

TABLEAU DE DIFFUSION : Référentiel Général de Sécurité. Version 1.2 – Janvier 2019

Destinataires		
Entité	Date de diffusion	Objet de la diffusion

TABLE DE L'HISTORIQUE DU DOCUMENT

Version	Date	Paragraphes et pages concernés	Objet de la mise à jour	Auteur
1.0	31/08/2018		Création	ANSSI
1.1	19/09/2018		Mise à jour	ANSSI
1.2	17/01/2019		Mise à jour	ANSSI

REMARQUE

Chaque révision du présent document doit correspondre à un numéro de version dont le format est : X. YY

Où X : est le numéro de version

Y : est le numéro de mise à jour de la version (indice de révision)

Une version nouvelle correspond à une modification majeure du contenu. Cette décision est prise lors de validation sur proposition de(s) l'auteur(s).

Table des matières

LISTE DES TABLEAUX

LISTE DES FIGURES

PREAMBULE

Le présent référentiel vise à établir un climat de confiance numérique dans un sous-espace du cyberespace burkinabè, à savoir celui concernant les services pilotés par les institutions gouvernementales et administratives, ainsi que les autres structures qui le désirent. Son objectif est de formaliser le Référentiel général de sécurité (RGS-BF) du Burkina Faso. Il prévoit un ensemble de règles pour que les systèmes d'information et de communication relatifs aux services du périmètre susmentionné fassent l'objet de sécurisation au cours des différentes phases de mise en œuvre. C'est ainsi que les mécanismes de protection prévus dans le RGS-BF sont applicables aussi bien aux systèmes d'information et de communication relatifs aux nouveaux services qu'à ceux relatifs aux services déjà déployés.

LISTE DES ACRONYMES

AC	:	Autorité de certification
AES	:	Advanced Encryption Standard
ANSSI	:	Agence nationale de sécurité des systèmes d'information
ARCEP	:	Autorité de régulation des communications électroniques et des postes
ASSI	:	Administrateur de la sécurité des systèmes d'information
CC	:	Critères communs
CC-NIST	:	Cadre de cybersécurité de NIST
CVE	:	Common vulnerabilities exposures
DPI	:	Dirigeant principal de l'information
EAL	:	Evaluation assurance levels
ESI	:	Electronic signatures and infrastructures
FISMA	:	Fédérale sur la gestion de la sécurité des informations
IDS	:	Systèmes de détection d'intrusions
ISATAP	:	Intra-site automatic tunnel addressing protocol
NIST	:	Institut national des standards et des technologies
PC	:	Politique de certification
PSAE	:	Prestataire de services d'archivage électronique
PSCE	:	Prestataire de services de certification électronique
PSCO	:	Prestataires de services de confiance
PSHE	:	Prestataire de services d'horodatage électronique
PSHO	:	Prestataire de services d'homologation
PSRE	:	Prestataire de services de recommandé électronique
PSSI	:	Politique de sécurité des systèmes d'information
RGS	:	Référentiel général de sécurité
RGS-BF	:	Référentiel général de sécurité du Burkina Faso
RSSI	:	Responsable de la sécurité des systèmes d'information
SI	:	Système d'information
SNCS-BF	:	Stratégie nationale de cybersécurité du Burkina Faso
SSI	:	Sécurité des systèmes d'information

GLOSSAIRE

1. **Atteinte à l'intégrité :** fait de provoquer intentionnellement une perturbation grave ou une interruption de fonctionnement d'un système d'information, d'un réseau de communications électroniques ou d'un équipement terminal, en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles des données.
2. **Audit de sécurité :** examen méthodique des composantes et des acteurs de la sécurité, de la politique, des mesures, des solutions, des procédures et des moyens mis en œuvre par une organisation, pour sécuriser son environnement, effectuer des contrôles de conformité, des contrôles d'évaluation de l'adéquation des moyens (organisationnels, techniques, humains, financiers) investis au regard des risques encourus, d'optimisation, de rationalité et de performance.
3. **Authentification** : action par laquelle le système d'information vérifie l'identité de l'usager. Les procédés utilisés par l'usager pour prouver son identité vont de l'emploi d'un couple identifiant/mot de passe à l'utilisation d'un certificat électronique personnel stocké sur une carte à puce.
4. **Autorité de certification :** autorité de confiance chargée de créer et d'attribuer des clés publiques et privées ainsi que des certificats électroniques.
5. **Autorité de Certification Racine :** organisme investi de la mission d'accréditation des autorités de certification, de la validation de la politique de certification des autorités de certification accréditées, de la vérification et de la signature de leurs certificats respectifs.
6. **BlockChain** : technologie de stockage et de transmission d'informations transparentes, sécurisées et fonctionnant sans organe central de contrôle.
7. **Confidentialité :** maintien du secret des informations et des transactions afin de prévenir la divulgation non autorisée d'informations aux non destinataires permettant la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert.
8. **Contenu :** ensemble d'informations relatives aux données appartenant à des personnes physiques ou morales, transmises ou reçues à travers les réseaux de communications électroniques et les Systèmes d'information.
9. **Contenu illicite :** contenu portant atteinte à la dignité humaine, à la vie privée, à l'honneur ou à la sécurité nationale.
10. **Cybercriminalité :** ensemble des infractions s'effectuant à travers le cyberspace par d'autres moyens que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique.
11. **Cyberdéfense :** ensemble des mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'information jugés essentiels . Le cadre de la cyberdéfense dépasse la simple sécurité informatique dans la mesure où elle a des conséquences directes sur la sécurité nationale et vient donc intéresser les différents organismes de Défense d'un pays. Avec la Lutte informatique défensive (LID) et la Lutte informatique offensive (LIO), la cyberdéfense permet de défendre et d'attaquer des ensembles de réseaux et ordinateurs qui contrôlent un pays.
12. **Cyberespace :** ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs.
13. **Cybersécurité :** ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres

actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes. Elle peut être également définie comme l'état recherché par un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

14. **Disponibilité :** critère de sécurité permettant que les ressources des réseaux de communications électroniques, des systèmes d'information ou des équipements terminaux soient accessibles et utilisables selon les besoins (le facteur temps).
15. **Données :** représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un équipement terminal, y compris un programme permettant à ce dernier d'exécuter une fonction.
16. **Données de connexion :** ensemble de données relatives au processus d'accès dans une communication électronique.
17. **Données à caractère personnel :** toute information qui permet, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques, notamment par référence à un numéro d'identification ou à plusieurs éléments spécifiques propres à leur identité physique, psychologique, psychique, économique, culturelle ou sociale.
18. **Exploitant de système d'information :** toute personne morale qui exploite un réseau de communications électroniques ouvert au public et / ou toute personne physique ou morale qui fournit un service de communications électroniques.
19. **Fiabilité :** aptitude d'un système d'information ou d'un réseau de télécommunications à fonctionner sans incident pendant un temps suffisamment long.
20. **Fournisseur d'accès ou FAI :** toute personne physique ou morale fournissant au public un accès à internet.
21. **Gravité de l'impact :** appréciation du niveau de gravité d'un incident, pondéré par sa fréquence d'apparition.
22. **Horodatage :** ce procédé permet de garantir qu'un document ou un message existait à un instant donné. Il fait foi dans le domaine des échanges électroniques.
23. **Infrastructures TIC critiques :** systèmes d'informations virtuels et physiques qui fournissent des services aux citoyens et servent de pivot à l'éclosion de la vie économique, sociale et sécuritaire du pays.
24. **Intégrité des données :** critère de sécurité définissant l'état d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal qui est demeuré intact et permet de s'assurer que les ressources n'ont pas été altérées (modifiées ou détruites) d'une façon tant intentionnelle qu'accidentelle, de manière à assurer leur exactitude, leur fiabilité et leur pérennité.
25. **Logiciel espion :** type particulier de logiciel trompeur collectant les informations personnelles (sites web les plus visités, mots de passe, etc.) auprès d'un utilisateur du réseau de communications électroniques.
26. **Logiciel potentiellement indésirable :** logiciel présentant des caractéristiques d'un logiciel trompeur ou d'un logiciel espion.
27. **Logiciel trompeur :** logiciel effectuant des opérations sur un équipement terminal d'un utilisateur sans informer préalablement cet utilisateur de la nature exacte des opérations que le logiciel va effectuer sur son équipement terminal ou sans demander à l'utilisateur s'il consent à ce que le logiciel procède à ces opérations.

28. **Opérations cybernétiques nationales :** emploi intégré des capacités cybernétiques pour des objectifs de la sécurité nationale.
29. **Organisme à infrastructures critiques** : une organisation identifiée par l'État comme ayant des activités indispensables ou dangereuses pour la population.
30. **Politique de sécurité :** référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser.
31. **Sécurité :** situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable, ou à en limiter les effets.
32. **Sécurité nationale :** stratégies prises par le pays pour assurer sa protection, y compris la prévention et la lutte contre les menaces internes et externes ainsi que d'autres actes susceptibles de menacer son intégrité.
33. **Signature électronique :** une donnée qui résulte de l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.
34. **Système de détection :** système permettant de détecter les incidents qui pourraient conduire aux violations de la politique de sécurité et permettant de diagnostiquer des intrusions potentielles.
35. **Système d'information :** dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, assurant par lui-même ou par un ou plusieurs de ses éléments, conformément à un programme, un traitement automatisé de données.
36. **TIC :** technologies de l'information et de la communication.
37. **Virus :** Programme malveillant destiné à endommager ou freiner le fonctionnement d'un système informatique.
38. **Vulnérabilité :** défaut de sécurité se traduisant soit intentionnellement, soit accidentellement par une violation de la politique de sécurité, dans l'architecture d'un réseau de communications électroniques, dans la conception d'un système d'information

INTRODUCTION

La protection du cyberespace repose non seulement sur la mise en œuvre efficiente de la Stratégie nationale de cybersécurité, mais également sur un ensemble de mécanismes de contrôle qui touche les activités sensibles. Il s'agit alors de s'assurer :

- que les solutions de sécurité déployées sont conformes à des exigences minimales de robustesse ;
- que les échanges électroniques mettant en jeu des données sensibles sont sécurisés en utilisant des mécanismes cryptographiques protégés selon un ensemble de procédures et de normes ;
- et que les risques relatifs aux systèmes d'information et de communication déployés sont identifiés et maîtrisés.

Un cadre unifié qui regroupe ces mécanismes est de nature à éviter les incohérences qui peuvent résulter dans leur mise en œuvre, surtout que les acteurs qui y seront impliqués sont multiples. Il permet en effet de bâtir une vision globale autour de laquelle s'articulent les règles et les recommandations de sécurité que doivent respecter les différentes étapes du cycle de vie d'un service déployé sur le cyberespace.

C'est dans cet ordre d'idées que ce document introduit le Référentiel général de sécurité du Burkina Faso (RGS-BF). Celui-ci s'inscrit dans l'objectif de créer un climat de confiance globale sur le cyberespace. La démarche adoptée pour mettre en œuvre le RGS-BF commence par un état des lieux à l'international où des expériences similaires sont analysées, notamment celle de la France. Ensuite, l'approche globale du RGS-BF est introduite. Il s'agit de définir le périmètre, les acteurs et les fonctions prévues pour élaborer les règles et les recommandations assurant le contrôle des services sensibles déployés. Les exigences relatives à ces fonctions sont ensuite détaillées selon une démarche basée sur la gestion des risques.

Ce présent document s'articule autour des points suivants :

- la première section revient sur les expériences internationales en matière de mise en œuvre de mécanismes de contrôle du cyberespace et se focalise sur l'expérience française puisqu'il s'agit du seul cas où le terme "référentiel général de sécurité" est utilisé ;
- la deuxième section élabore une conception du RGS-BF et introduit son contenu;
- la troisième section décrit les dispositions définies par le RGS-BF en matière de gestion des risques de sécurité ;

- la quatrième section définit les dispositions définies par le RGS-BF en matière de sécurisation des transactions électroniques. Les exigences relatives à la cryptologie, les fonctions de sécurité et les prestataires de service de confiance sont citées à ce niveau ;
- la cinquième section est consacrée aux dispositions en matière d'homologation et de certification des solutions de sécurité ;
- la sixième section traite la protection des systèmes d'information et les exigences relatives aux aspects sous-jacents en matière de processus d'audit et de gestion des incidents ;
- la septième section donne le processus de suivi du RGS-BF.

1 ETAT DES LIEUX A L'INTERNATIONAL

Cette section donne un aperçu sur certaines expériences à l'international en termes de référentiels de sécurité. La première section est consacrée aux Référentiel général de sécurité (RGS) français alors que la seconde section analyse les équivalents dans les contextes américains et français.

1.1 LE RGS DANS LA REGLEMENTATION FRANÇAISE

Le terme "référentiel général de sécurité" existe exclusivement au niveau de la réglementation française. Il a été prévu par l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives. Il consiste en un ensemble de règles et de recommandations relatives aux fonctions de sécurité réparties sur les étapes de la démarche suivante :

1. réalisation d'une analyse des risques ;
2. définition des objectifs de sécurité ;
3. choix et mise en œuvre des mesures appropriées de protection et de défense du SI;
4. homologation de sécurité du Système d'information (SI) ;
5. suivi opérationnel de la sécurité du SI.

Une première version (RGS 1.0) a été publiée en mai 2010 et une deuxième version (RGS 2.0) en mai 2014.

Le RGS 2.0 comporte les documents suivants :

- Référentiel général de sécurité.
- Annexe A1 – Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques.
- Annexe A2–Politique de Certification Type "certificats électroniques de personne".
- Annexe A3 – Politique de Certification Type "services applicatifs".
- Annexe A4 – Profils de certificats, CRL, OCSP et algorithmes cryptographiques.
- Annexe B1–Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.
- Annexe B2 – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques.
- Annexe B3–Règles et recommandations concernant les mécanismes d'authentification.
- Annexe C – Référentiel d'exigences applicables aux prestataires d'audit de la SSI.

1.2 EQUIVALENTS A L'INTERNATIONAL

Cette sous-section traite deux (02) exemples de réglementations où le terme RGS n'apparaît pas, mais qui portent sur des champs d'application similaires. Il s'agit du cas des Etats-Unis d'Amérique et du Canada.

1.2.1 Loi fédérale sur la gestion de la sécurité des informations (FISMA)

La loi Fédérale sur la gestion de la sécurité des informations (FISMA) est une loi américaine adoptée en 2002 et faisant partie du *E-Gouvernement Act* de 2002 qui est défini pour améliorer la gestion des services et des processus électroniques des administrations publiques. Cette loi impose aux agences fédérales de développer, documenter et mettre en œuvre un programme de sécurité et de protection de l'information et ceci dans le but de réduire les risques de sécurité liés aux données fédérales. Afin d'aboutir à ces objectifs, FISMA a établi un ensemble de directives et de normes de sécurité que les organismes fédéraux doivent respecter. Elle s'applique à tout organisme public administrant des programmes fédéraux ainsi qu'à toute structure privée impliquée dans une relation contractuelle avec le gouvernement. FISMA a défini un cadre règlementaire de conformité avec les standards *Institut National des Standards et des Technologies*, *Etats-Unis* (NIST). Les exigences de cette loi se résument aux points suivants :

- Inventaire des systèmes d'information : chaque agence doit établir l'inventaire des systèmes d'information qu'elle héberge ainsi que leurs interfaces. Dans ce cadre le référentiel NIST SP 800-18 fournit un guide pour la définition du périmètre des systèmes d'information.
- Catégorisation des risques: les agences en question doivent classifier leurs informations et systèmes d'information par niveau de risque conformément à la norme FIPS 199.
- Planification : toute agence concernée doit élaborer une politique de planification de la sécurité de son système d'information. Ceci doit se faire conformément au référentiel NIST SP-800-18. Les plans de Sécurité des systèmes d'information (SSI) sont des documents qui nécessitent une révision périodique afin d'être mis à jour dans le but de proposer des actions pour l'implémentation des mesures de sécurité.
- Mesures de sécurités : le référentiel NIST 800-53 fournit un catalogue complet de mesures de sécurité à mettre en œuvre pour la conformité avec FISMA. Cependant, la loi n'impose pas que l'intégralité de ses mesures soit implémentée par chaque institution, mais il s'agit de choisir celles qui répondent à ses besoins en matière de sécurité.

- Evaluation des risques : c'est une composante élémentaire des exigences de FISMA. Le référentiel NIST SP 800-30 fournit un ensemble de directives détaillant le processus d'évaluation des risques. Selon ce référentiel, l'évaluation des risques concerne le niveau organisationnel, les processus métier et les systèmes d'information.
- Certification et Accréditation : FISMA exige que les responsables des agences concernées veillent à ce que l'évaluation des risques soit effectuée chaque année au sein de leurs agences afin de garantir que le niveau des risques reste réduit. Pour qu'elle soit certifiée et accréditée FISMA, une agence fédérale doit suivre le processus planification, certification, accréditation et suivi continu.

1.2.2 Pratique recommandée en sécurité de l'information au Québec

Afin de mettre en œuvre une gouvernance forte et intégrée de la sécurité de l'information gouvernementale, le Québec a établi un guide de pratiques recommandées en sécurité de l'information. Ce guide répond à l'obligation du Dirigeant principal de l'information (DPI) d'accompagner les organismes publics et de leur apporter le soutien nécessaire dans la prise en charge des exigences de sécurité de l'information gouvernementale, notamment par l'élaboration et la diffusion de guides, pratiques et outils en la matière.

La mise en œuvre de ce guide est appuyée par les éléments suivants :

- la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement ;
- la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics ;
- la directive sur la sécurité de l'information gouvernementale, le cadre gouvernemental de gestion de la sécurité de l'information, le Cadre de gestion des risques et des incidents à portée gouvernementale, et l'approche stratégique gouvernementale 2014-2017 en sécurité de l'information qui définissent le cadre de gouvernance de la sécurité de l'information dans l'administration québécoise;
- la politique de sécurité de l'information de l'organisme public concerné.

Le guide québécois des pratiques recommandées comprend les documents suivant :

- le guide d'élaboration d'une politique de sécurité ;
- le guide d'élaboration d'un cadre de gestion de la sécurité de l'information ;
- le guide d'audit de la sécurité de l'information ;
- le guide de catégorisation de l'information ;
- le guide d'intrusions et de vulnérabilités ;
- le guide d'élaboration et de mise en œuvre d'un processus de gestion des risques de sécurité de l'information ;

- le guide d'élaboration d'un tableau de bord de sécurité de l'information ;
- le guide établissant les critères de désignation des principaux intervenants en sécurité de l'information ;
- le guide de gestion des accès logiques ;
- le guide de sensibilisation à la sécurité de l'information ;
- le guide d'utilisation sécuritaire des assistants numériques personnels.

Le guide s'applique à l'information gouvernementale consignée dans un document, tel que décrit à l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1). L'information visée est celle qu'un organisme public détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

2 APPROCHE DU RGS-BF

Cette section présente le contexte du RGS-BF. Elle traite du périmètre, décline la démarche méthodologique et décrit la constitution du document.

2.1 CONTEXTE DU REFERENTIEL GENERAL DE SECURITE DU BURKINA FASO

2.1.1 Périmètre du RGS-BF

Le Référentiel général de sécurité du Burkina Faso (RGS-BF) vise à établir un climat de confiance numérique dans un périmètre défini par deux (02) dimensions :

- une dimension institutionnelle spécifiant les entités comprises dans ce périmètre ;
- une dimension fonctionnelle spécifiant les fonctions soumises aux dispositions du référentiel.

Le périmètre institutionnel comporte lui-même un périmètre interne et un périmètre externe tel que l'illustre la Figure 1 :

- Le périmètre interne (représenté en jaune) comporte les institutions qui déploient des systèmes d'information et de communication sur le cyberespace et qui appartiennent à l'une des catégories suivantes :
  - Ministères, institutions gouvernementales et autres structures relevant de l'administration (établies physiquement au Burkina Faso ou à l'étranger).
  - Opérateurs de télécommunications.
  - Fournisseurs d'accès Internet.
  - Sociétés opérant dans le développement et la commercialisation des solutions de sécurité.

- Institutions financières (banques, microfinances, assurances, institutions de gestion de portefeuilles électroniques, …).
- Organismes à infrastructure critique.
- Organes indépendants dont le rôle est lié à la gouvernance, à la régulation et à la souveraineté de l'Etat.

✧ Le périmètre externe regroupe trois (03) catégories d'entités (représentées par trois (03) nuances de vert) :

- Les Prestataires de services de confiance (PSCO) accrédités au sens du RGS-BF (autorités de certification et autorités d'horodatage remplissant les exigences de l'Annexe STE-2).
- Les entités accréditées à exercer des activités d'homologation
- Les auditeurs de sécurité des systèmes d'information et de communication accrédités au sens du RGS-BF (remplissant les exigences de l'Annexe PRO-3).

La différenciation entre les deux (02) périmètres s'explique par le fait que les entités qui y appartiennent jouent des rôles différents par rapport à la sécurité du cyberespace. En effet, les entités faisant partie du périmètre interne hébergent des services dont la sensibilité est élevée (car leur périmètre est large ou car les classes de sécurité d'information qu'ils gèrent est élevée) alors que les entités du périmètre externe jouent un rôle actif dans la sécurisation des entités du périmètre interne.

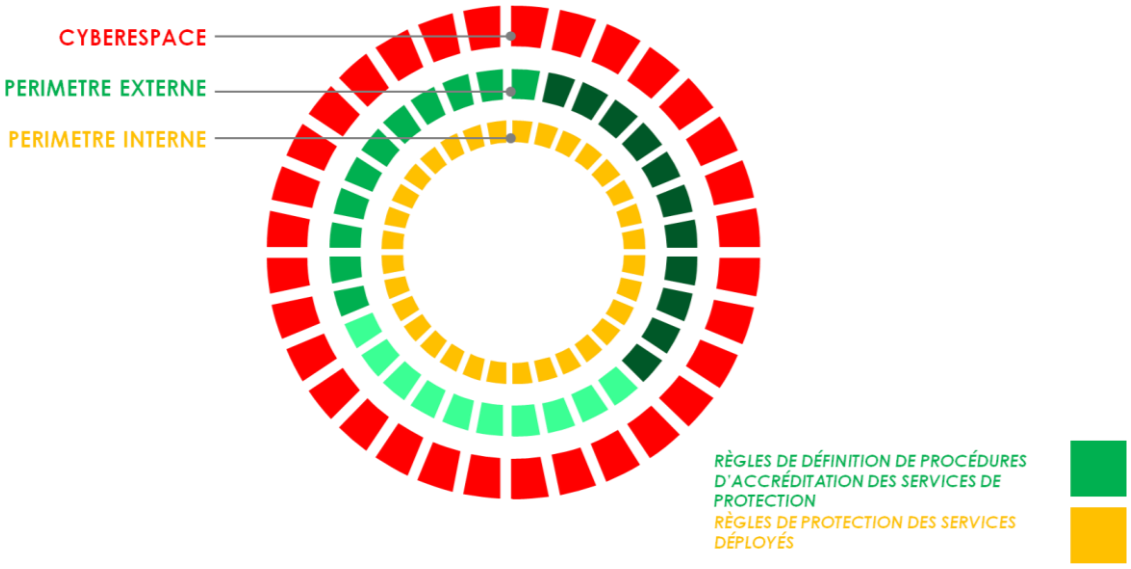

Figure 1 : Périmètre fonctionnel du RGS-BF.

Cette différenciation est encore visible à travers les périmètres fonctionnels s'appliquant aux périmètres interne et externe.

Ainsi, le périmètre fonctionnel appliqué au périmètre interne comprend des règles et des recommandations visant à protéger les processus suivants :

- La génération, le traitement, l'échange, le stockage et l'archivage des informations dans le cadre de services pilotés par des entités du périmètre interne et ciblant les utilisateurs finaux.
- La génération, le traitement, l'échange, le stockage et l'archivage des informations dans le cadre de services établis entre plusieurs entités du périmètre interne.

Le périmètre fonctionnel appliqué au périmètre externe comprend l'application de règles et de recommandations visant à accréditer les entités jouant un rôle actif dans l'instauration de la confiance dans le cyberespace. Il s'agit notamment des points suivants :

- L'accréditation des prestataires de services de confiance.
- L'accréditation des prestataires de services d'audit de sécurité.

Dans ce qui suit, le terme périmètre du RGS-BF désigne l'union des périmètres interne et externe.

2.2 DEMARCHE DU RGS-BF

Le RGS-BF est complémentaire à la Stratégie nationale de cybersécurité du Burkina Faso (SNCS-BF). Il prévoit un ensemble de règles et de recommandations pour que les systèmes d'information et de communication relatifs aux services du périmètre interne fassent l'objet de sécurisation au cours des différentes phases de mise en œuvre et que les entités du périmètre externe soient accréditées. Ainsi, ces règles et recommandations doivent être réparties sur les étapes de la démarche aboutissant à déployer un service sur le cyberespace. C'est d'ailleurs le cas du RGS français dont la démarche est toutefois particulière et n'émane pas d'un standard.

Il convient aussi de noter que les mécanismes de protection prévus dans le RGS-BF sont applicables aussi bien aux systèmes d'information et de communication relatifs aux nouveaux services qu'à ceux relatifs aux services déjà déployés. Dans ce cadre, le RGS-BF permet notamment :

- de favoriser l'adoption par son périmètre de bonnes pratiques en matière de sécurité des systèmes d'information ;
- d'adapter les solutions techniques aux contextes de sécurité identifiés pour chaque système d'information faisant partie du périmètre désigné ci-dessus ;
- d'offrir aux entités du périmètre RGS-BF les labels de sécurité permettant de s'assurer de la qualité des solutions de sécurité qu'ils ont à déployer .

Pour une répartition rigoureuse des règles et des recommandations du RGS-BF, le cycle de vie du déploiement d'un service sur le cyberespace est représenté en utilisant les étapes du référentiel NIST en matière de gestion des risques. Il s'agit d'un cadre structuré, ci-après noté NIST-RMF, qui permet de conduire des missions de gestion des risques des systèmes d'information et de communication en intégrant une panoplie d'outils, de techniques et de standards internationaux. Le cycle de vie du NIST-RMF comporte six (06) étapes détaillées ci-après :

1. Catégorisation : consiste à recenser les informations traitées, enregistrées ou communiquées dans le cadre des processus métier informatisés.
2. Sélection : consiste à sélectionner un ensemble initial de contre-mesures sur la base d'une analyse des risques.
3. Déploiement : consiste à mettre en place les contre-mesures retenues lors de l'étape précédente.

4. Evaluation : consiste à estimer que les solutions sont déployées correctement, c'est-à-dire si elles opèrent conformément aux objectifs fixés, et si elles donnent les résultats escomptés.
5. Autorisation : consiste à accepter le fonctionnement du système avec les contre-mesures sélectionnées et avec le niveau de risque résiduel.
6. Suivi : consiste à assurer le contrôle continu de l'efficacité et l'efficience des contre-mesures déployées.

L'utilisation de ces étapes pour concevoir la démarche du RGS-BF est en parfaite cohérence avec la disposition qui vise à généraliser l'usage de ce référentiel dans le périmètre interne (conformément aux dispositions de l'Annexe GRE-1).

Les règles et les recommandations du RGS-BF sont classées en six (06) catégories :

1. Gestion des risques de sécurité.
2. Sécurisation des transactions électroniques.
3. Homologation des solutions de sécurité.
4. Protection préventive des systèmes d'information et de communication.
5. Protection réactive des systèmes d'information et de communication.
6. Suivi de la sécurité des systèmes d'information et de communication.

La répartition de ces catégories sur les étapes du NIST-RMF est donnée dans la Figure 2.

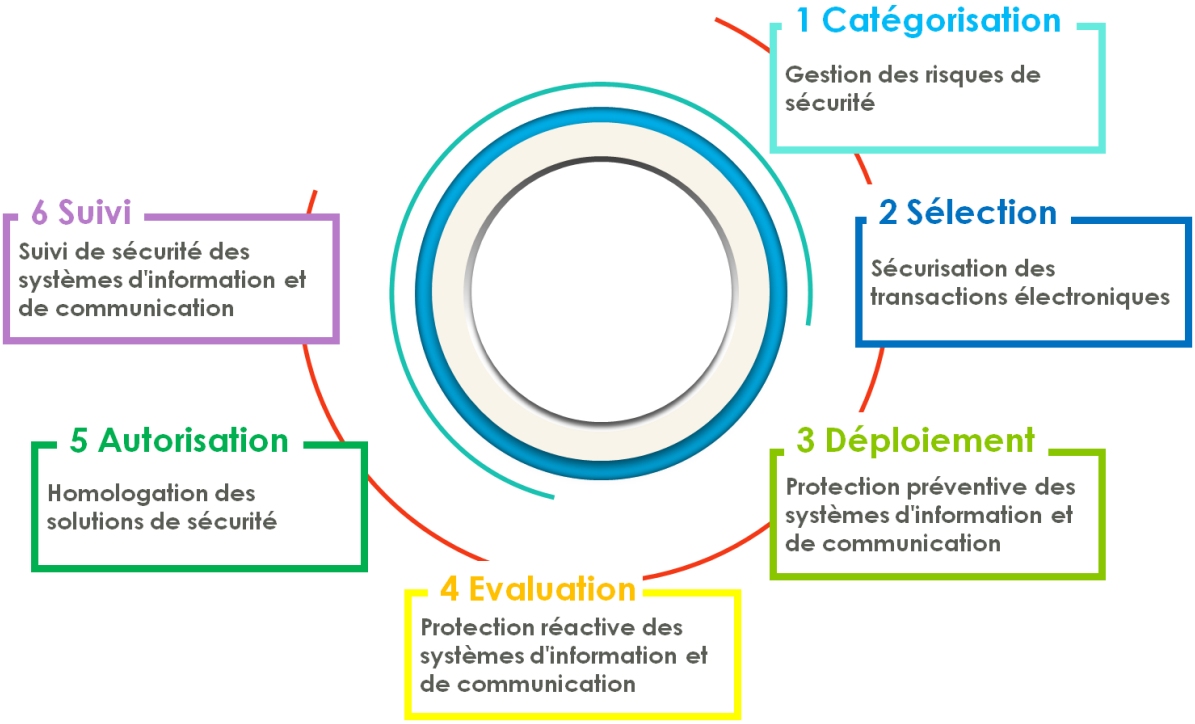

Figure 2 : Répartition des catégories du RGS-BF.

2.3 CONSTITUTION DU REFERENTIEL GENERAL DE SECURITE DU BURKINA FASO

Le RGS-BF se compose d'un ensemble de sections et d'annexes. Pour une bonne présentation, chaque section du RGS-BF fait l'objet d'une numérotation et comprend une description et un ensemble de règles et de recommandations mises en encadré.

Les détails techniques se rapportant aux règles et aux recommandations sont mis en annexe. C'est ainsi que le présent document comprend les annexes listés ci-dessous.

Code	Annexe
GRE-1	Exigences relatives au processus de gestion des risques de sécurité
GRE-2	Exigences relatives à l'analyse des risques de sécurité dans un contexte interne
GRE-3	Exigences relatives à l'analyse des risques de sécurité dans le contexte national
STE-1	Exigences relatives à la gestion des clés cryptographiques
STE-2	Exigences relatives à l'accréditation des prestataires de services de confiance
STE-3	Exigences relatives aux politiques de certification
HOM-1	Exigences relatives à l'homologation des solutions de sécurité
PRO-1	Exigences relatives à la protection proactive des systèmes d'information et de communication
PRO-2	Exigences relatives à la protection réactive des systèmes d'information et de communication
PRO-3	Exigences relatives à l'accréditation des auditeurs des systèmes d'information et de communication

3 GESTION DES RISQUES DE SECURITE

Cette section définit les dispositions du RGS-BF en matière de gestion des risques. Deux (02) aspects sont alors abordés :

- La gestion des risques : il s'agit d'un processus structuré permettant d'établir une cartographie des risques présents dans un systèmes d'information et de communication, de classer ces risques par ordre d'importance et d'établir un plan de traitement de risques en conséquence. Le RGS-BF prévoit des dispositions dans ce contexte afin de faciliter le traitement des rapports de risques collectés au sein de son périmètre interne.
- L'analyse des risques : elle constitue une sous-étape du processus de gestion des risques. Son objectif est de cartographier les risques présents dans un périmètre spécifique. Le RGS-BF prévoit des dispositions spécifiques relativement à cette étape (et non pour les autres étapes du processus de gestion des risques) et ceci dans un souci de faciliter la compilation des cartographies de risques établis par les entités faisant partie du périmètre interne et de respecter la gouvernance interne de ces entités en laissant une liberté de choix au niveau des détails techniques et des mécanismes de décision (basée sur le risque).

3.1 PROCESSUS DE GESTION DES RISQUES

L'objectif de la gestion des risques est d'identifier, d'analyser et de cartographier les risques de sécurité d'un système d'information et de communication. Généralement, un processus de gestion des risques est composé de cinq (05) étapes principales :

1. Documentation du système : consiste à identifier le périmètre du système et à collecter la documentation concernant les processus, l'information et les moyens de communication faisant partie du système analysé. Durant cette étape, des entretiens avec le personnel de la structure sont menés pour aboutir à une liste de ressources classifiées par ordre de sensibilité de l'information qu'elles contiennent ou échangent. Les échelles d'impact et de probabilité sont ensuite établies en déterminant le nombre de niveaux et les seuils de passage d'un niveau vers un autre ainsi que la correspondance entre ces niveaux et la sévérité des risques sous-jacents. Ceci sert à évaluer la sévérité des risques qui seront identifiés lors de la deuxième étape. En outre, les solutions de sécurité déjà implémentées sont documentées à ce niveau afin qu'elles soient tenues en considération lors de la proposition de nouvelles contre-mesures.

2. Analyse des menaces et des vulnérabilités : des questionnaires et des test d'intrusion sont réalisés à ce niveau pour identifier les vulnérabilités qui existent dans les ressources identifiées lors de l'étape précédente. Les menaces qui correspondent à ces vulnérabilités sont ensuite analysées à travers l'attribution d'un niveau d'impact et de probabilité à chacune d'entre elles.
3. Analyse des risques : les résultats obtenus lors de la deuxième étape sont compilés en vue d'attribuer un niveau de risque pour chaque couple (menace, ressource). Les risques identifiés sont ensuite classés selon leur ordre de sévérité.
4. Proposition d'un plan de traitement des risques : en fonction des niveaux de sévérité obtenus après l'étape 3, des stratégies de traitement de risques sont proposées en fonction de la sévérité de ceux-ci. Les stratégies sont classifiées en quatre (04) types majeurs :
    a. Accepter : s'applique aux risques dont le niveau de sévérité est bas.
    b. Eviter : s'applique aux risques dont les niveaux de probabilité et d'impact sont très élevés.
    c. Réduire : s'applique aux risques dont le niveau de probabilité est élevé alors que le niveau d'impact est faible.
    d. Transférer : s'applique aux risques dont le niveau d'impact est élevé alors que le niveau de probabilité est faible.

    Des contre-mesures potentielles sont proposées à ce niveau comme des alternatives possibles pour l'implémentation des stratégies mentionnées ci-dessus.
5. Suivi des risques : l'évolution du traitement des risques identifié fait l'objet d'un suivi continu pour prendre en considération l'avancement en matière de mise en œuvre des mécanismes de protection prévus. Ainsi, une échelle d'états de risque ainsi qu'une échelle d'états de traitements doit être élaborée à cet effet.

Règle 1. Le RGS-BF impose la réalisation d'une mission de gestion des risques une fois tous les deux (02) ans pour les entités du périmètre RGS-BF.

Règle 2. Chaque entité du périmètre RGS-BF est tenue d'avoir une cartographie des risques faisant l'objet d'un suivi continu.

Recommandation 1. La méthodologie recommandée par le RGS-BF pour la conduite de la gestion des risques est celle du référentiel de gestion des risques NIST-RMF, conduite selon les dispositions de l'Annexe GRE-1.

Règle 3. Le standard NIST-RMF est recommandé et il n'est pas imposé par le RGS-BF. Il est toutefois imposé que la gestion des risques prévue dans la règle 1 soit, à défaut de la méthode NIST-RMF, basée sur les standards COBIT5 et ISO/IEC 27001-8.

Règle 4. Toute cartographie des risques basée sur un autre référentiel sera considérée non conforme aux dispositions du RGS-BF.

Dans le but de faciliter aux structures l'utilisation de ces standards en préservant l'interopérabilité et l'homogénéité des solutions de sécurité déployées, un tableau de correspondance est donné dans l'Annexe 1 du RGS-BF.

3.2 ANALYSE DES RISQUES

L'analyse des risques consiste à traduire les menaces et les vulnérabilités présentes au niveau d'un système d'information et de communication déployé par une entité du périmètre RGS-BF en risques aptes à être évalués. Dans un contexte interne à l'entité bénéficiaire, elle est réalisée dans la perspective d'améliorer les processus de prise de décision liés à la sécurité des systèmes d'information et de communication. Dans le contexte national, elle vise à dresser un profil national de sécurité du cyberespace.

Dans ce contexte, le RGS-BF définit deux (02) cas d'application de la phase d'analyse des risques :

1. Analyse de risques dans le contexte interne : ce cas d'application s'inscrit dans le cadre d'un processus de gestion des risques dont le périmètre est un système d'information et de communication déployé par une entité. L'analyse des risques est alors élaborée selon le processus NIST-RMF dont les dispositions sont précisées dans la sous-section précédente. Les dispositions prévues pour cette analyse des risques permettent de garantir une uniformité des cartographies des risques qui seront collectées par l'Agence nationale de sécurité des systèmes d'information (ANSSI) tous les deux (02) ans. Les cartographies élémentaires seront utilisées en interne (par les entités bénéficiaires) pour établir un plan de traitement de risques et à l'échelle nationale par l'ANSSI pour établir une cartographie nationale des risques.
2. Analyse de risques dans le contexte national : ce cas d'application s'inscrit dans le cadre d'un processus visant à établir un état des lieux de la sécurité du cyberespace à l'échelle nationale. Des rapports de diagnostic élémentaires collectées auprès des entités faisant du périmètre du RGS-BF sont alors traitées par l'ANSSI pour dresser un profil de risque du cyberespace national. Cet état des lieux est élaboré chaque

année. Les résultats de cet état des lieux ne font pas foi d'une cartographie des risques et ne peuvent pas être utilisés pour élaborer un plan de traitement des risques.

Les règles du RGS-BF par rapport à ces deux (02) cas d'application sont données dans les deux (02) sous-sections suivantes.

3.2.1 Analyse de risques dans le contexte interne

L'objectif de l'analyse de risques interne est d'allouer un niveau de risques à chaque menace présente sur un système d'information et de communication. Le RGS-BF définit quatre (04) règles relatives aux dimensions de risque, à l'échelle de fréquence, à l'échelle d'impacts et à l'échelle des risques.

3.2.1.1 Dimensions de risque

Les risques identifiés pour un systèmes d'information et de communication sont analysés selon, au moins, les trois (03) dimensions suivantes :

1. Confidentialité : restreindre l'accès à l'information aux entités autorisées. Ceci englobe la protection des informations personnelles et touchant la propriété intellectuelle.
2. Intégrité : préserver l'information contre les modifications non autorisées. Ceci englobe la non-répudiation des actions réalisées par le moyen de l'information en question et l'authenticité de celle-ci.
3. Disponibilité : assurer l'accès fiable et à temps à l'information. Cet accès doit en même temps être réservé aux entités autorisées.

Règle 5. Les entités du périmètre RGS-BF doivent utiliser les dimensions "Confidentialité", "Intégrité" et "Disponibilité" dans l'élaboration des cartographies des risques dans leur contexte interne.

3.2.1.2 Echelle de fréquences

La fréquence traduit la probabilité d'occurrence des menaces. Elle renseigne essentiellement sur le nombre de fois qu'une vulnérabilité risque d'être exploitée au cours d'un intervalle de temps. Le RGS-BF définit cinq (05) niveaux de fréquence donnés notés par **A**, **B**, **C**, **D**, et **E**. Il s'agit d'une échelle de cinq (05) niveaux allant des menaces rares jusqu'à celles dont l'occurrence est presque certaine.

Règle 6. Les entités du périmètre RGS-BF doivent fixer les valeurs **F1**, **F2**, **F3**, **F4** et **F5** qui correspondent aux cinq (05) niveaux **A**, **B**, **C**, **D**, et **E** dans l'élaboration des échelles de fréquence dans leur contexte interne et ce conformément aux dispositions de l'Annexe GRE-2-1.

3.2.1.3 Echelle d'impacts

Le RGS-BF définit trois (03) niveaux d'impact (**faible**, **moyen**, **haut**) pour chacun des objectifs de sécurité (confidentialité, intégrité, disponibilité). Des valeurs **I1**, **I2** et **I3** seront définies par l'entité bénéficiaire pour chaque mission d'analyse des risques.

Règle 7. Les entités du périmètre RGS-BF doivent fixer les valeurs **I1**, **I2** et **I3** qui correspondent aux échelles d'impact **faible**, **moyen** et **haut** dans leur contexte interne et ce conformément aux dispositions de l'Annexe GRE-2-2.

Recommandation 2. Il est recommandé de réviser les valeurs à chaque démarrage d'une mission de gestion des risques.

3.2.1.4 Echelle de risques

Les niveaux d'impact et de probabilité sont utilisés pour définir une échelle de risques qui sera utilisée pour classifier les risques qui seront identifiés dans le système d'information et de communication. L'échelle définie par le RGS-BF comporte quatre (04) niveaux de risques :

- **Faible (F)** : Les risques de cette catégorie seront acceptés comme étant des risques résiduels.
- **Moyen (M)** : Les risques de cette catégorie seront réduits par le moyen du renforcement des mesures de sécurité d'ordre documentaire, organisationnel, ou technique.
- **Important (I)** : Les risques de cette catégorie seront transférés au vu de l'impact important qu'ils risquent de générer en cas d'occurrence des menaces qui en sont l'origine.
- **Critique (C)** : Les risques de cette catégorie seront évités car ils affectent des missions critiques de la structure.

Ces niveaux sont attribués par l'entité bénéficiaire selon des règles d'association entre les niveaux de fréquence et les niveaux d'impact qu'elle définit pour chaque mission d'analyse des risques.

Règle 8. Les entités du périmètre RGS-BF doivent élaborer des échelles de risques en associant les niveaux de fréquence **A**, **B**, **C**, **D**, et **E**, les niveaux d'impact **faible**, **moyen** et **haut** et les niveaux de risque **faible**, **moyen**, **important** et **critique**, et ce conformément aux dispositions de l'Annexe GRE-2-3.

3.2.2 Analyse de risques dans le contexte national

L'analyse de risques nationale se matérialise par une contribution de l'ensemble des structures pour un diagnostic annuel de la sécurité du cyberespace, élaboré par l'ANSSI. Le format imposé est celui du Cadre de cybersécurité de NIST (CC-NIST). Selon ce cadre, cinq (05) dimensions (appelées aussi fonctions) sont utilisées pour évaluer le niveau de sécurité du cyberespace. Ces dimensions sont :

1. Identification : cette dimension traduit la capacité des acteurs à cerner les éléments du contexte national de cybersécurité et les ressources sur lesquelles reposent les fonctions sensibles et critiques.
2. Protection : cette dimension traduit la capacité des systèmes déployés sur le cyberespace à limiter l'impact des menaces qui y sont présentes. Les mécanismes de protection mis en place sont la gestion d'identité, le contrôle d'accès, la sensibilisation et la formation, la sécurité des données, la sécurité des processus, la maintenance et les technologies de protection.
3. Détection : cette dimension traduit la capacité des systèmes déployés sur le cyberespace à assurer la détection fiable des incidents de sécurité. Les catégories des mécanismes dans cette dimension sont les processus de détection, la gestion des anomalies et des incidents de sécurité et le suivi de l'état de sécurité des systèmes.
4. Réponse : cette dimension traduit la capacité des systèmes déployés sur le cyberespace à assurer la réponse aux incidents de sécurité. Il s'agit donc d'évaluer le degré de préparation de ces systèmes à affronter les menaces et ceci en termes de planification des réponses, de communication sur les incidents de sécurité, d'analyse des incidents, de traitement des incidents et d'amélioration de la sécurité des systèmes visés.
5. Restauration : cette dimension traduit la capacité des systèmes déployés sur le cyberespace à assurer la restauration des composantes ayant été la cible

d'incidents de sécurité. Cette capacité s'exprime en termes de planification des activités de restauration, de la communication sur ces activités et d'améliorations faisant suite à la récupération.

Le RGS-BF prévoit la soumission obligatoire, une fois par an, d'une évaluation des risques à l'ANSSI. Sur la base des contributions collectées, un profil cible sera défini pour le cyberespace pour l'année en question. Les questions considérées par le RGS-BF pour constituer le rapport soumis par une structure est donné dans l'Annexe 2. Il s'agit de 98 questions réparties sur les fonctions d'indentification, de protection, de détection, de réaction et de restauration. Le niveau de risque est traduit par les échelles suivantes :

- **Application partielle (AP)** : les pratiques de gestion des risques ne sont pas formalisées et les décisions sont prises ad hoc.
- **Risque communiqué (RC)** : les pratiques de gestion des risques sont approuvées par la hiérarchie mais ne font pas l'objet d'une politique formalisée.
- **Répétable (R)** : les pratiques de gestion des risques sont approuvées et formalisées.
- **Adaptative (A)** : les pratiques de gestion des risques sont approuvées, formalisées et ont fait l'objet d'une évaluation sur la base d'un nombre d'indicateurs de performance.

Les principales références documentaires qui ont servi pour le développement de ces guides d'entretien pour chaque dimension sont donnés dans le **Tableau 1**.

Tableau 1 : Références utilisées pour le diagnostic de l'état de sécurité du cyberespace.

Etape	Référentiels
Identification	NIST 800-100: Information Security Handbook: A Guide for Managers NIST 800-35: Guide to Information Technology Security Services NIST 800-39 : Managing Information Security Risk: Organization, Mission, and Information System View
Détection	NIST 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations NIST 1800-7 : Situational Awareness for Electric Utilities
Protection	NIST 800-64 Rev. 2: Security Considerations in the System Development Life Cycle NIST 800-160 : Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
Réponse	NIST 800-34 Rev. 1 : Contingency Planning Guide for Federal Information Systems
Restauration	NIST 800-184 : Guide for Cybersecurity Event Recovery

4 SECURISATION DES TRANSACTIONS ELECTRONIQUES

Les règles techniques imposées par le RGS-BF portent uniquement sur la sécurisation des infrastructures utilisées pour procéder aux échanges électroniques entre les différentes structures et les usagers ainsi qu'entre les structures elles-mêmes.

Le RGS n'impose aucune technologie particulière et laisse aux différentes structures le choix des mesures à mettre en œuvre. Il fixe cependant des exigences relatives à certaines fonctions de sécurité, notamment la certification, l'horodatage et l'audit.

En fonction de leur besoin de sécurité, issu de l'analyse de risques, il appartient aux structures de déterminer les fonctions de sécurité ainsi que les niveaux de sécurité associés, en s'appuyant sur les méthodes, les outils et les bonnes pratiques proposés dans le RGS-BF.

Lorsqu'elles choisissent de mettre en œuvre des fonctions de sécurité traitées dans la présente section, les structures choisissent le niveau de sécurité adapté à leur besoin et appliquent les règles correspondantes décrites dans ce référentiel.

4.1 REGLES RELATIVES A LA CRYPTOLOGIE

Les mécanismes cryptographiques sont couramment utilisés pour la protection des transactions électroniques. Le RGS-BF définit un ensemble de règles et de recommandations relativement à la cryptologie. Ces règles et recommandations portent sur les aspects suivants :

- définition des catégories d'algorithmes cryptographiques ;
- spécification des conditions permettant de garantir de la robustesse des algorithmes considérés contre la cryptanalyse ;
- spécifications des mécanismes permettant de gérer les clés cryptographiques en maîtrisant le risque lié à leur exposition.

4.1.1 Catégories d'algorithmes cryptographiques

Un algorithme de cryptage est généralement constitué d'un espace de textes clairs, un espace de clés, un espace de textes chiffrés, une fonction de cryptage et une fonction de décryptage. Les usages possibles d'un algorithme de cryptage sont liés aux fonctions de sécurité dont notamment la confidentialité, l'intégrité, l'authentification et la non-répudiation. Selon les exigences de sécurité relatives aux services déployés par les entités bénéficiaires, le RGS-BF prévoit trois (03) catégories d'algorithmes cryptographiques tel que le stipule la règle suivante.

Règle 9. Trois (03) catégories d'algorithmes cryptographiques sont reconnues par le RGS-BF. Il s'agit des algorithmes de cryptage symétrique, des algorithmes de cryptage asymétrique et des fonctions de hachage. Ces catégories sont définies dans l'Annexe STE-1-1.

Recommandation 3. Les algorithmes de chiffrement symétrique suivants sont :

- AES-128
- AES-192
- AES-256
- 3TDEA

Ces algorithmes sont définis dans l'Annexe STE-1-2.

Règle 10. Les entités du périmètre RGS-BF utilisant des algorithmes de cryptage asymétrique doivent s'assurer qu'ils sont basés sur l'un des problèmes suivants :

- Problème de factorisation
- Problème du logarithme discret dans les corps finis
- Problème de logarithme discret dans le corps des courbes elliptiques

Règle 11. L'usage d'un algorithme de cryptage asymétrique conforme au RGS-BF est imposé pour l'émission d'une signature numérique.

Recommandation 4. Les algorithmes de cryptage asymétrique recommandés par le RGS-BF sont :

- RSA
- ECDSA

Ces algorithmes sont définis dans l'Annexe STE-1-3.

Recommandation 5. Les fonctions de hachage recommandées par le RGS-BF sont :

- SHA-256
- SHA-384
- SHA-512

Ces algorithmes sont définis dans l'Annexe STE-1-4.

4.1.2 Robustesse contre la cryptanalyse

Des règles et des recommandations sont prévues par le RGS-BF pour assurer la robustesse des algorithmes cryptographiques utilisés contre la cryptanalyse (ensemble de techniques permettant de déduire un texte clair ou une clé cryptographique sans respecter les procédés définis par l'algorithme qui lui correspond). Ces règles énumèrent, pour les algorithmes de cryptage définis par le RGS-BF, les dispositions qui garantissent la résistance de ces algorithmes par rapport à un ensemble de procédés de cryptanalyse. Ces règles sont données ci-dessous. Elles se réfèrent à des paramètres des algorithmes cryptographiques qui sont définis dans les Annexes STE-1-1, STE-1-2, STE-1-3 et STE-1-4.

Règle 12. Lors de l'usage d'un algorithme de cryptage symétrique, la taille de la clé utilisée doit être supérieure à 128 bits. De plus, aucune attaque réussie contre l'algorithme nécessitant moins de 2^{128} opérations de calcul ne doit exister.

Règle 13. Lors de l'usage d'un algorithme de cryptage symétrique par bloc, les règles suivantes doivent être respectées :

- la taille d'un bloc doit être supérieure à 128 bits ;
- aucune attaque contre le mode opératoire de chiffrement nécessitant moins de 2^{56} appels de la primitive cryptographique ne doit exister.

Règle 14. Lors de l'usage d'un algorithme de cryptage asymétrique basé sur le problème de factorisation, les règles suivantes doivent être respectées :

- la taille du module et de l'exposant privé doit être supérieure à 2048 bits ;
- la taille de l'exposant public doit être supérieure à 2^{16}.

Règle 15. Lors de l'usage d'un algorithme de cryptage asymétrique basé sur le problème du logarithme discret dans les corps finis, les règles suivantes doivent être appliqués :

- le module du groupe utilisé doit être premier ;
- la taille du module doit être supérieure à 2048 bits.

Règle 16. Lors de l'usage d'un algorithme de cryptage symétrique basé sur le problème du logarithme discret dans les courbes elliptiques, l'ordre des sous-groupes utilisé doit être supérieur à 256 bits.

Règle 17. Lors de l'usage de fonctions hachage, les règles suivantes doivent être respectées :

- la taille du condensé doit être supérieure à 256 bits ;
- la résistance de la fonction de hachage à la collision, au sens du standard FIPS 180-4, doit être supérieure à 128 bits ;

- la résistance primaire de la fonction de hachage à l'inversion, au sens du standard FIPS 180-4, doit être supérieure à 256 bits ;

- la résistance secondaire de la fonction de hachage à l'inversion, au sens du standard FIPS 180-4, doit être supérieure à 256 bits.

4.1.3 Gestion des clés

Les clés faisant partie des algorithmes cryptographiques peuvent être utilisées à des fins diverses. Etant donné qu'elles représentent un élément sensible lors de l'utilisation des algorithmes cryptographiques, leur usage doit faire l'objet de mesures spécifiques. Le critère utilisé dans le RGS-BF pour définir les mesures de protection selon les cas d'usage des clés est la cryptopériode (définie dans le document NIST 800-57pt1-r4).

Le RGS-BF établit un ensemble de cas d'usage des clés et spécifie, pour chacun de ces cas d'usage, une règle relative à la cryptopériode.

Règle 18. Les cas d'usage des clés reconnus dans le RGS-BF sont :

- clé privée de signature ;
- clé publique de signature ;
- clé symétrique d'authentification ;
- clé privée d'authentification ;
- clé publique d'authentification ;
- clé symétrique de chiffrement de données ;
- clé symétrique de chiffrement de clé ;
- clés symétriques pour RBG ;
- clé maître symétrique ;
- clé privée pour le transport de clé ;
- clé publique pour le transport de clé ;
- clé symétrique pour l'échange de clé ;
- clé privée pour l'échange de clé ;
- clé publique pour l'échange de clé ;
- clé privée unique pour l'échange de clé ;
- clé publique unique pour l'échange de clé ;
- clé symétrique d'autorisation ;

- clé privée d'autorisation ;

- clé publique d'autorisation.

Ces cas d'usage sont définis dans l'Annexe STE-1-5.

Règle 19. Les cryptopériodes qui doivent être respectées pour chaque cas d'usage sont données dans l'Annexe STE-1-6.

4.2 ACCREDITATION DES PRESTATAIRES DE SERVICES DE CONFIANCE

4.2.1 Champ d'application

Les certificats électroniques délivrés dans le périmètre du RGS-BF doivent être conformes à un ensemble de règles et de recommandations.

La procédure de vérification concerne les certificats mis en œuvre dans le but d'assurer les fonctions de sécurité suivantes :

- Authentification d'une personne et d'un serveur.
- Signature électronique et cachet.
- Confidentialité.

Conformément aux politiques de certification types mentionnées ci-dessus, la procédure de délivrance de certificats recouvre les aspects suivants :

- l'identification et la vérification de l'identité des agents à qui seront délivrés des certificats ;
- la fabrication technique des certificats ;
- la remise des certificats aux porteurs ;
- la publication (ou mise à disposition) des certificats, de leur statut et de la politique de certification ;
- la révocation et le renouvellement des certificats.

Lorsqu'elle met en place une procédure de délivrance de certificats, une structure s'appuie sur une Autorité de certification (AC) interne ou externe, qui peut être publique ou privée.

Une AC peut elle-même recourir à des prestataires externes pour la mise en œuvre de certaines des fonctions mentionnées. Dans tous les cas, la structure reste seule responsable du processus global de délivrance.

Lorsqu'elle recourt à une AC externe, la structure doit établir des procédures qui lui permettent de s'assurer du respect, par cette AC, des règles du présent paragraphe.

Règle 20. Un Prestataire de services de confiance (PSCO), défini au sens de la loi 45/2009, doit être accrédité par l'Autorité de régulation des communications électroniques (ARCEP) selon les dispositions de l'Annexe STE-2-1. Il doit aussi être conforme aux exigences des dispositions des articles 82 à 88 et 108 à 124 de la loi 45/2009.

Règle 21. Des exigences spécifiques sont définies pour les catégories de PSCO définies dans la loi 45/2009. Il s'agit de :

- Prestataire de services de certification électronique (PSCE) : doit remplir les exigences d'un PSCO et être conforme aux exigences des dispositions des articles 108 à 145 de la loi 45/2009.

- Prestataire de services d'horodatage électronique (PSHE) : doit remplir les exigences d'un PSCO et être conforme aux exigences des dispositions des articles 98 à 101 de la loi 45/2009 ;

- Prestataire de services d'archivage électronique (PSAE) : doit remplir les exigences d'un PSCO et être conforme aux exigences des dispositions des articles 89 à 97 de la loi 45/2009 ;

- Prestataire de services de recommandé électronique (PSRE) : doit remplir les exigences d'un PSCO et être conforme aux exigences des dispositions des articles 102 à 107 de la loi 45/2009.

Règle 22. Les PSCO accrédités doivent faire l'objet, tous les trois (03) ans, d'un audit réalisé par l'ARCEP pour renouveler l'accréditation. Cet audit est réalisé selon les dispositions de l'Annexe STE-3-2.

4.3 REGLES ET RECOMMANDATIONS RELATIVES A LA PROTECTION DES ECHANGES ELECTRONIQUES

Le RGS-BF prévoit quatre (04) fonctions pour la protection des échanges électroniques sur le cyberespace. Il s'agit de la confidentialité, l'authentification, la signature électronique et l'horodatage. Cette section est consacrée aux règles et aux recommandations visant à assurer la bonne utilisation de ces fonctions. Vu l'importance que jouent les certificats électroniques dans la protection de ces fonctions, une première sous-section est dédiée aux exigences relatives aux certificats électroniques déployés sur le cyberespace burkinabè.

4.3.1 Règles relatives aux certificats électroniques

Les exigences du RGS-BF relatives aux certificats électroniques portent sur le contenu des certificats, sur les conditions de leur émission par un Prestataire de services de confiance (PSCO), et sur le dispositif de stockage des clés privées correspondantes.

Règle 23. Le format des certificats électroniques utilisés par les entités faisant partie du périmètre du RGS-BF doit être conforme aux standards suivants :

- Les champs du certificat doivent être utilisés en conformité avec le standard X.509 ;
- Les champs du certificat doivent respecter les exigences spécifiques mentionnées dans l'Annexe STE-3-4.

Le RGS-BF offre la possibilité de disposer :

- ✧ des certificats mono-usage à usage d'authentification de personne physique ou de serveur, de signature, de cachet et de confidentialité pour les classes 1, 2 3 et 3+ définis dans les Annexes 2 et 3 ;
- ✧ d'un certificat électronique unique, dit à usage multiple, assurant les fonctions d'authentification de personne physique et de signature électronique. Ce certificat est limité aux classes 1 et 2 des Annexes 2 et 3.

4.3.2 L'authentification d'une entité par certificat électronique

L'authentification désigne la vérification d'une identité utilisée sur le cyberespace. Une telle identité peut être associée à une personne (exemple : adresse e-mail, nom d'utilisateur) ou à un nœud déployé sur le réseau (exemple : adresse URL, adresse IP). Ainsi, le RGS-BF prévoit deux (02) fonctions d'authentification, à savoir l'authentification des personnes et l'authentification des serveurs.

Règle 24. Deux (02) types de certificats d'authentification sont reconnus au sens du RGS-BF :

- Certificat d'authentification personnel : l'identité indiquée dans le certificat se base sur un attribut personnel ;
- Certificat d'authentification serveur : l'identité indiquée dans le certificat se base sur une adresse de serveur.

Règle 25. Trois (03) classes sont définies pour chaque type de certificat d'authentification. La désignation de ces classes est donnée dans l'Annexe STE-3-5.

4.3.3 La signature et le cachet électroniques

La signature électronique d'une personne permet de garantir l'identité du signataire, l'intégrité du document signé et le lien entre le document signé et la signature. Elle traduit ainsi la manifestation du consentement du signataire quant au contenu des informations signées.

Dans le cas des échanges dématérialisés faisant intervenir des services applicatifs, la fonction de « cachet » permet de garantir l'intégrité des informations échangées et l'identification du service ayant « cacheté » ces informations. Cette fonction de « cachet » est, pour une machine, l'équivalent de la fonction signature pour une personne.

La mise en œuvre par une structure, des fonctions de sécurité « signature électronique » ou « cachet » peut se faire selon trois (03) niveaux de sécurité aux exigences croissantes des classes 1, 2 et 3. Ces exigences, décrites dans l'annexe 2, couvrent, pour les trois (03) classes, l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, à savoir :

- ✧ la paire de clés et le certificat électronique dont l'usage est la signature électronique ou le cachet ;
- ✧ le dispositif de création de signature électronique ou de cachet ;
- ✧ l'application de création de signature électronique ou de cachet ;
- ✧ le module de vérification de signature électronique ou de cachet.

4.3.4 La confidentialité

Le chiffrement constitue le mécanisme essentiel de protection de la confidentialité. Cependant, la confidentialité des informations peut aussi être protégée par des mesures complémentaires de gestion des droits d'accès de chacun (en lecture, en écriture ou en modification) aux données contenues dans le système d'information. À cet effet, il est recommandé de mettre en place des mécanismes techniques afin de s'assurer que seules les personnes autorisées puissent accéder aux données en fonction de leur besoin d'en connaître. Ces mécanismes doivent être robustes et implémentés au plus près du lieu de stockage des données.

La mise en œuvre par une structure, de la fonction de sécurité « Confidentialité » peut se faire selon trois (03) niveaux de sécurité aux exigences croissantes des classes 1, 2 et 3.

Ces exigences, décrites dans l'annexe 2, couvrent, pour les trois (03) classes de certificats, l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, à savoir :

- la paire de clés et le certificat électronique dont l'usage est le chiffrement ;
- le dispositif de chiffrement ;
- le module de chiffrement ;
- le module de déchiffrement.

4.3.5 Règles relatives à l'horodatage électronique

Les exigences concernant le composant « contremarque de temps » sont décrites dans l'annexe 3 du RGS-BF. Elles portent sur le contenu des contremarques de temps et sur les conditions dans lesquelles il est émis par un Prestataire de services d'horodatage électronique (PSHE).

Une fonction d'horodatage permet d'attester qu'une donnée sous forme électronique existe à un instant donné. Cette fonction met en œuvre une contremarque de temps générée à l'aide d'un mécanisme cryptographique respectant les règles et les recommandations contenues dans le RGS-BF.

Cette contremarque, délivrée par un Prestataire de services d'horodatage électronique (PSHE), doit respecter les exigences de la Politique de Certification Type. Celle-ci ne définit qu'un niveau unique de sécurité, auquel les autorités administratives doivent se conformer dès lors qu'elles souhaitent mettre en œuvre la fonction d'horodatage électronique au sein de leur système d'information.

4.4 TECHNOLOGIES BLOCKCHAIN ET SECURITE DES TRANSACTIONS ELECTRONIQUES

La blockChain est une technologie de stockage et de transmission d'informations transparentes, sécurisées et fonctionnant sans organe central de contrôle.

Techniquement, il s'agit d'une base de données distribuées dont les informations envoyées par les utilisateurs et les liens interne à la base sont vérifiés et groupés à intervalle de temps régulier, en blocs, l'ensemble étant sécurisé par cryptographie et formant ainsi une chaine. Elle peut être aussi vue sous un autre angle comme une base de données distribuée sur différents nœuds de stockage. Ces nœuds de stockage ce sont les utilisateurs qui vont apporter à l'aide des machines de la puissance de calcul de l'espace de stockage pour faire fonctionner la blockchain.

Les chaînes de blocs peuvent contribuer à protéger l'information en garantissant l'intégrité et l'authenticité des données et fichiers, tout au long de leur cycle de vie.

Vulgarisée à partir de 2008 avec l'avènement des crypto-monnaies (et du bitcoin en particulier), la technologie de la chaîne de blocs, plus connue sous le nom de blockchain, a été taillée pour orchestrer et fiabiliser les transactions virtuelles. Elle s'articule autour d'une sorte de grand livre de compte informatisé et distribué à travers un réseau. De par son caractère décentralisé, une blockchain permet de s'assurer de l'intégrité et de l'historique des transactions.

Outre les crypto-monnaies, les systèmes de blockchain sont désormais de plus en plus sollicités pour sécuriser d'autres types d'actifs virtuels. Les cas d'application sont multiples :

- ✧ signature électronique des documents financiers ;
- ✧ sécurisation des titres de propriété foncière ;
- ✧ sécurisation des diplômes dans le secteur éducatif ;
- ✧ etc.

Plus globalement, tout document dématérialisé ou toute donnée transitant par un système d'informations pourrait bénéficier d'une blockchain pour être certifié et tracé. L'objectif étant, au final, de doter le contenu d'un certificat susceptible de le protéger contre toute modification non-autorisée, et ce tout au long de son cycle de vie. Ainsi la technologie des Blockchains pourrait contribuer à résoudre plusieurs enjeux de sécurité :

- ✧ intégrité des données ;
- ✧ protection contre des attaques DDoS ;
- ✧ authentification.

La technologie blockchain a pour fondement : l'horodatage des blocs de données minés, se reposant sur une paire de clés, publique et privée et aussi l'absence d'un tiers de confiance.

Comme exigences inhérentes à la blockchain :

Recommandation 6.	Prendre en compte les exigences en matière d'horodatage (STE-3-2 : Critères techniques).
Recommandation 7.	Tenir compte des exigences en matière de cryptographie (Annexes A4, B1 et B2).
Recommandation 8.	Mettre en oeuvre un mecanisme de chifrrement conformement aux points Annexes STE-1-1, STE-1-2, STE-1-3 et STE-1-4.
Recommandation 9.	Considerer les aspects legaux et reglementaires en vigueur.

5 HOMOLOGATION DES SOLUTIONS DE SECURITE

L'homologation des solutions de sécurité permet de donner une assurance des propriétés de sécurité qu'elles respectent. Elles permettent aussi de renseigner d'une manière rationnelle sur les risques résiduels qui correspondent à son utilisation. Ainsi, une entité chargée de l'homologation (appartenant au périmètre externe du RGS-BF) doit rendre accessible aux acteurs du cyberespace les informations relatives à la robustesse d'une solution de sécurité par rapport à un ensemble d'exigences définies au préalable. Le RGS-BF prévoit des règles et des recommandations pour trois (03) cas de figure :

- ✧ L'homologation des solutions de sécurité par rapport à une spécification.
- ✧ L'homologation des implantations de mécanismes cryptographiques dans les solutions de sécurité.
- ✧ L'homologation par rapport à la robustesse aux vulnérabilités.

En outre, des dispositions relatives au rôle de Prestataire de services d'homologation (PSHO) sont prévues dans cette section.

Règle 26. Trois (03) types d'homologation de solutions de sécurité sont définis dans le RGS-BF :

- L'homologation relative à une spécification.
- L'homologation de la robustesse des implantations cryptographiques.
- L'homologation relative à une liste de vulnérabilités.

Règle 27. Le rôle du Prestataire de services d'homologation (PSHO) est assuré par l'ANSSI.

Règle 28. Une solution de sécurité est homologuée si elle est évaluée par le PSHO selon la démarche donnée dans l'Annexe HOM-1-1.

Règle 29. Pour chaque solution de sécurité, et pour chaque type d'homologation, trois (03) niveaux d'homologation sont définis :

- Niveau basique.
- Niveau moyen
- Niveau robuste

Les règles d'attribution de ces niveaux sont données dans l'Annexe HOM-1-2.

6 PROTECTION DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

6.1 PROTECTION PREVENTIVE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

La protection préventive des systèmes d'information et de communication présente de nombreuses différences par rapport à l'approche réactive. Plutôt que d'attendre que les problèmes se présentent avant d'y répondre, le principe de cette approche est de minimiser la possibilité qu'ils se produisent dès le départ. Pour protéger les ressources importantes de votre entreprise, vous devez mettre en place des contrôles visant à réduire les risques d'exploitation des vulnérabilités par des programmes ou des personnes malveillantes ou par un usage erroné non intentionnel.

Les mécanismes de protection préventive comprennent des mesures de nature :

- Technique: produits de sécurité (matériels ou logiciels), outils de confiance basés sur les certificats numériques.
- Organisationnelle : organisation des responsabilités (habilitation du personnel, obligation d'homologation des produits informatiques avant toute exploitation (tout ce qui intervient dans un système d'information informatisé), gestion des ressources humaines (affectation d'agents responsables de la gestion du système d'information, formation du personnel spécialisé, sensibilisation des utilisateurs).

Ces mesures de sécurité peuvent être sélectionnées au sein des référentiels et normes existants. Elles peuvent également en être adaptées par un effort d'intégration ou bien être développées et par conséquent personnalisées.

Règle 30. Les prestataires de services d'audit doivent être accrédités selon les dispositions prévues dans l'Annexe PRO-1-1.

Règle 31. Chaque entité du périmètre RGS-BF est tenue de faire auditer ses systèmes d'information et de communication une fois chaque deux (02) ans.

Recommandation 10. Il est recommandé aux entités du périmètre RGS-BF de mettre en œuvre des systèmes firewalls et des systèmes de prévention de codes malveillants selon les dispositions des Annexes PRO-1-2 et PRO-1-3.

6.2 PROTECTION REACTIVE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

La protection réactive des systèmes d'information et de communication consiste à adopter un traitement pondéré et rationnel des incidents de sécurité de manière à capitaliser un savoir-faire permettant d'acquérir une meilleure immunité face à des incidents. Ceci requiert la maîtrise d'un processus à quatre (04) étapes :

1. Contenir les dégâts : En contenant les dommages infligés par l'attaque, ils est possible de limiter l'étendue de ces dommages. Il est vital de protéger rapidement les données, logiciels et matériel sensibles. Il peut être risqué de laisser les systèmes visés par les incidents connectés en cas d'attaque, car ceci peut à terme entraîner des problèmes de plus grande ampleur. Ceci est notamment le cas des vers. Toutefois, le fait de déconnecter les serveurs infectés, bien qu'il permet de confiner l'impact du ver dans un périmètre relativement réduit, peut s'avérer encore plus néfaste que l'incident lui-même. C'est ainsi que les décisions prises par les équipes de réponse aux incidents doivent faire l'objet d'une analyse poussée pour prendre la bonne décision sans pour autant que cette décision soit prise une fois que les dégâts deviennent irréversibles. L'expérience de ces équipes et leur connaissance des systèmes d'information et de communication permet de déterminer alors l'utilité de chaque alternative et d'en sélectionner celle qui correspond à l'état des systèmes victimes. En outre, des copies des configurations et des fichiers journaux devront être gardées pour faciliter la récupération (troisième étape).
2. Evaluer les dégâts : une fois que la situation maîtrisée, il faut déterminer dès que possible l'ampleur des dommages causés par l'incident de sécurité. Cette étape est cruciale, car elle permet de remettre en place les systèmes fonctionnels tout en conservant une copie des systèmes pour pouvoir les analyser. Dans le cas où cette évaluation n'est pas possible, il faut mettre en œuvre un plan de réserve qui permettra de poursuivre une activité normale et de conserver un certain niveau de productivité. En outre, c'est à ce stade que les pilotes des systèmes d'information et de communication ayant fait l'objet de l'incident peuvent engager une procédure judiciaire auprès des autorités judiciaires.
3. Réparer les dégâts : afin de déterminer l'origine de l'attaque, il est crucial de comprendre quelles ressources étaient visées et quelles faiblesses ont été exploitées pour obtenir l'accès ou perturber les services. Entre autres, il faut examiner la configuration du système, le niveau de correction, les journaux systèmes et les journaux d'audit sur les systèmes directement affectés et sur les périphériques réseau acheminant leur trafic. Cet examen permet de découvrir l'origine de l'attaque au niveau du système et les ressources ayant été affectées. Les dégâts sont ensuite réparés en utilisant des mécanismes de récupération qui dépendent de la nature des systèmes visés et des mécanismes de disponibilité et de conservation utilisés.
4. Mettre à jour les mécanismes de protection : une fois que les phases de documentation et de récupération ont été effectuées, il est nécessaire d'examiner l'ensemble du processus. L'équipe de réponse aux incidents détermine les étapes

exécutées correctement et les erreurs commises. Il faudra alors mettre à jour quelques processus de façon à mieux appréhender les incidents futurs. Ceci est fait en identifiant et évaluant les faiblesses dans le plan de réponse aux incidents. L'intérêt de cet exercice a posteriori est de rechercher les possibilités d'amélioration. L'analyse des failles permet en effet d'insuffler de nouveaux principes de planification des réponses aux incidents et de gérer ceux-ci plus efficacement.

Règle 32. Chaque entité du périmètre RGS-BF est tenue, en cas d'occurrence d'un incident de sécurité dans un système d'information et de communication qu'elle déploie, d'engager un processus de réponse aux incidents conforme aux dispositions de l'Annexe PRO-2-1.

Recommandation 11. Il est recommandé aux entités du périmètre RGS-BF de mettre en œuvre des systèmes de détection et de préventions des intrusions et des systèmes de prévention de codes malveillants selon les dispositions des Annexes PRO-2-2 et PRO-2-3.

6.3 INTELLIGENCE ARTIFICIELLE ET PROTECTION DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

Les solutions d'intelligence artificielle peuvent contribuer à la protection préventive des systèmes d'information.

L'intelligence artificielle est un domaine scientifique qui s'intéresse à la recherche de solutions à des problèmes complexes, comme le feraient les humains. Un mécanisme de décision similaire à celui d'un humain est utilisé et modélisé avec certains algorithmes. Le Machine Learning est un sous-domaine de l'intelligence artificielle. Le Machine Learning utilise des méthodes mathématiques et statistiques pour extraire des informations à partir de données. Avec cette information, le machine Learning tente de deviner l'inconnu. Le Deep Learning est un sous-domaine du Machine Learning qui essaie de comprendre les données avec une approche de réseau neuronal artificiel.

Le but des applications d'intelligence artificielle est de résoudre en très peu de temps un problème complexe sur lequel un expert passerait énormément de temps.

Dans le domaine de la sécurité informatique, l'intelligence artificielle peut avoir plusieurs applications :

- Applications de filtrage anti-spam.
- Détection et prévention des intrusions sur le réseau.
- Détection de fraude.
- Détection de botnet.

- Authentification utilisateur sécurisée.
- Cotes de cybersécurité.
- Prévision des incidents de piratage.
- Etc.

7 SUIVI DE SECURITE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

Les mesures de protection d'un système d'information et de communication doivent être accompagnées d'un suivi opérationnel régulier ainsi que de mesures de surveillance et de détection, afin de réagir au plus vite aux incidents de sécurité et de les traiter au mieux.

Le suivi opérationnel consiste à appliquer les mécanismes de gestion des incidents et d'utiliser les outils de protection réactive prévus dans l'Annexe PRO-2 du RGS-BF.

Au-delà de l'analyse de risques et de l'homologation, le RGS-BF recommande l'adoption de bonnes pratiques relatives à la méthodologie, aux procédures et à l'organisation.

7.1 ORGANISER LA SECURITE DES SYSTEMES D'INFORMATION

7.1.1 Organiser les responsabilités liées à la sécurité des systèmes d'information

Les structures doivent mettre en œuvre une organisation qui endosse les responsabilités liées à la sécurité des systèmes d'information.

De préférence dirigée par un représentant de la structure , cette organisation doit disposer des moyens matériels nécessaires à la réalisation de ses missions et de la capacité à gérer les risques, les crises ou les incidents qui pourraient en résulter. Le cas échant, elle s'appuie sur une chaîne fonctionnelle de sécurité chargée de l'assister dans le pilotage, la gestion et le suivi des moyens SSI. Cette chaîne fonctionnelle est composée :

- d'un Responsable de la sécurité des systèmes d'information (RSSI) ;
- d'un Administrateur de la sécurité des systèmes d'information (ASSI) ;
- d'un correspondant SSI ;
- etc.

Éventuellement à l'aide de la chaîne fonctionnelle SSI, l'organisation mise en place par la structure peut assurer les missions suivantes :

- coordination des actions permettant l'intégration des clauses liées à la SSI dans les contrats ou les conventions impliquant un accès par des tiers à des informations ou à des ressources informatiques ;
- formalisation de la répartition des responsabilités liées à la SSI (définition des périmètres de responsabilité, des délégations de compétences, etc.) ;

- établissement des relations nécessaires avec les autorités externes de défense des systèmes d'information, notamment pour la gestion des intrusions et des attaques sur les systèmes.

7.1.2 Mettre en place un système de management de la sécurité des systèmes d'information

Il est recommandé de mettre en œuvre des processus permettant de rechercher une amélioration constante de la SSI. Par exemple, la mise en place d'un système de management de la sécurité de l'information, tel que défini dans la norme ISO 27001, permet non seulement de planifier et de mettre en œuvre les mesures de protection du système d'information, mais également d'en vérifier la pertinence et la conformité par rapport aux objectifs établis.

7.1.3 Élaborer une politique de sécurité des systèmes d'information

Il est recommandé d'élaborer et de formaliser une Politique de sécurité des systèmes d'information (PSSI).

Elle peut être générale ou déclinée en fonction des besoins spécifiques de chaque domaine de chaque système d'information.

7.1.4 Impliquer les instances décisionnelles

Les instances décisionnelles des structures doivent être impliquées dans la sécurisation des systèmes d'information dont elles ont in fine la responsabilité, afin de donner les orientations adéquates, notamment en termes d'investissement humain et financier, et de valider les objectifs de sécurité et les orientations stratégiques. La norme ISO 27001 fournit, à titre indicatif, une liste de sujets susceptibles d'être traités au niveau de la direction de la structure.

7.2 ADAPTER L'EFFORT DE PROTECTION DES SYSTEMES D'INFORMATION AUX ENJEUX DE SECURITE ET PRENDRE EN COMPTE LA SSI DANS LES PROJETS

La sécurité d'un système d'information doit être adaptée aux enjeux du système lui-même et aux besoins de sécurité de la structure, afin d'y consacrer les moyens financiers et humains nécessaires et suffisants. Dans ce but, il convient d'utiliser les recommandations qui permettent, dans le cadre du développement d'un projet de système d'information, de déterminer les enjeux relatifs à la sécurité et d'identifier l'ensemble des livrables relatifs à la SSI.

7.2.1 Adopter une démarche globale

L'ensemble de la démarche de sécurisation des systèmes d'information doit procéder d'une volonté cohérente et globale, afin d'éviter la dispersion des efforts des équipes en

charge de la SSI ou la mise en œuvre de mesures de sécurité parcellaires. Chaque décision doit être prise au juste niveau hiérarchique. Il est ainsi recommandé :

- de prendre en considération tous les aspects qui peuvent affecter la SSI, qu'ils soient techniques (matériels, logiciels, réseaux) ou non (organisations, infrastructure, personnel) ;
- d'envisager tous les risques et menaces, quelle que soit leur origine ;
- de prendre en compte la SSI à tous les niveaux hiérarchiques. La SSI repose sur une vision stratégique et nécessite des choix d'autorité (enjeux, moyens humains et financiers, risques résiduels acceptés) ainsi qu'un contrôle des actions et de leur légitimité ;
- de responsabiliser tous les acteurs (décideurs, maîtrise d'ouvrage et d'œuvre, utilisateurs) ;
- d'intégrer la SSI tout au long du cycle de vie des systèmes d'information (depuis l'étude d'opportunité jusqu'à la fin de vie du système).

D'une manière similaire, la sécurité doit être prise en compte dès la phase de définition des objectifs fonctionnels des systèmes d'information, afin de :

- limiter les surcoûts inhérents à l'application tardive de mesures de sécurité ;
- garantir l'efficacité des mesures mises en œuvre ;
- favoriser l'appropriation de la sécurité par les équipes en charge du SI.

7.2.2 Informer et sensibiliser le personnel

L'ensemble des agents d'une structure, et le cas échant les contractants et les utilisateurs tiers, doivent suivre une formation adaptée sur la sensibilisation et recevoir régulièrement les mises à jour des politiques et des procédures qui concernent leurs missions. Cette formation doit permettre de réduire les risques liés à la méconnaissance des principes de base et des règles élémentaires de bonne utilisation de l'outil informatique.

La sensibilisation du personnel doit être régulière. À cet effet, l'ANSSI publie des bonnes pratiques pour l'application de principes de base en matière de sécurité des systèmes.

7.2.3 Prendre en compte la sécurité dans les contrats et les achats

Les exigences de sécurité relatives aux produits ou aux prestations acquis doivent faire l'objet d'une étude et doivent être clairement formalisées et intégrées dans les dossiers d'appels d'offres, au même titre que les exigences fonctionnelles, réglementaires, de performance ou de qualité.

Ces exigences peuvent concerner le système qui fait l'objet de la consultation, mais aussi la gestion du projet lui-même (formation ou habilitation des personnels), en incluant les phases opérationnelles et de maintenance. Il convient notamment de :

- veiller à intégrer aux règlements de consultation ou aux cahiers des charges les référentiels de l'ANSSI applicables (produits certifiés, qualifiés, agréés…) ;
- demander à ce que les produits de sécurité soient fournis avec l'ensemble des éléments permettant d'en apprécier le niveau de sécurité ;
- préciser les clauses relatives à la maintenance des produits acquis ;
- préciser les clauses concernant les conditions de l'intervention et de l'accès physique et logique des sous-traitants ;
- préciser les clauses garantissant la qualité et la sécurité des prestations et produits fournis ;
- préciser les conditions de propriété des codes sources ;
- prévoir, le cas échéant, la réversibilité des prestations et la portabilité des données générées pendant celles-ci en s'assurant en particulier que les bases de données sont extractibles, que celle-ci peut être distinguée du système lui-même et que les formats utilisés sont ouverts ;
- préciser la nature et les modalités de réalisation des tableaux de bord et mécanismes de suivi des prestations de sécurité ;
- prévoir les modalités de réaction aux crises et aux incidents susceptibles d'affecter le système ;
- prévoir des points de contact compétents à même de répondre aux besoins des structures ;
- vérifier, dans les réponses à appel d'offres, la couverture des exigences sécurité inscrites dans la consultation.

Une attention particulière devra être portée aux mécanismes de validation et de recette des composants mettant en œuvre les exigences de sécurité.

7.2.4 Prendre en compte la sécurité dans les projets d'externalisation et d'informatique en nuage

Le recours à l'externalisation ou à « l'informatique en nuage » présente des risques spécifiques qu'il convient d'évaluer avant d'aborder une telle démarche. Ces risques peuvent être liés au contexte même de l'opération d'externalisation ou à des spécifications contractuelles déficientes ou incomplètes. Dans cette hypothèse, il est recommandé d'appliquer les démarches suivantes :

- une démarche cohérente de prise en compte des aspects SSI lors de la rédaction du cahier des charges d'une opération d'externalisation ;
- un ensemble de clauses types ainsi qu'une base d'exigences de sécurité, à adapter et à personnaliser en fonction du contexte particulier de chaque projet d'externalisation.

7.2.5 Mettre en place des mécanismes de défense des systèmes d'information

En complément des mécanismes de protection des systèmes d'information, et en fonction de leurs enjeux de sécurité, les structures doivent adopter des mesures complémentaires relatives à la défense des systèmes d'information. Ces mesures consistent, en particulier, à assurer :

- la connaissance des systèmes exploités par la structure, ou en relation avec elle(cartographie des SI, répertoire des interconnexions, etc.);
- la détection des malveillances, des erreurs et des imprudences, en périphérie ou à l'intérieur des systèmes d'informations des structures ;
- la traçabilité des actions et des accès réalisés sur les systèmes d'information (journalisation, notamment) ;
- la pérennisation des savoir-faire et des compétences, notamment en termes d'exploitation des SI ;
- la conservation de la preuve des infractions découvertes.

7.2.6 Utiliser les produits et prestataires homologués pour leur sécurité

L'homologation permet d'attester de la confiance que l'on peut accorder à des produits de sécurité et à des Prestataires de services de confiance(PSCO), ainsi que de leur conformité aux règles du RGS-BF qui leurs sont applicables. D'autres labels existent pour attester de la compétence des professionnels, notamment en matière de SSI.

Ainsi, il est recommandé :

- d'utiliser chaque fois que possible des produits de sécurité homologués ;
- de recourir chaque fois que possible à des PSCO qualifiés ;
- de prendre en considération, pour le choix des prestataires, en plus de leur qualification, leur éventuelle certification selon la norme ISO 27001 ou d'autres normes équivalentes ;
- de prendre en considération, pour le choix de prestataires, la certification de leurs personnels lorsque des compétences particulières sont requises pour une fonction.

7.2.7 Élaborer des plans de traitement d'incidents ainsi que de continuité et de reprise d'activité

Les structures doivent se préparer à faire face à des incidents de sécurité pour lesquels toutes les mesures préventives auraient échoué. A ce titre, elles doivent mettre en œuvre un plan de continuité d'activité et un plan de reprise d'activité qui identifient les moyens et les procédures nécessaires pour revenir à une situation nominale le plus rapidement possible, en cas d'incident grave. Ces documents doivent être régulièrement mis à jour. Les plans et les procédures qui en découlent doivent faire l'objet de tests réguliers.

7.2.8 Procéder à des audits réguliers de la sécurité du système d'information

Les structures doivent réaliser ou faire réaliser des audits réguliers de leurs SI. À cet effet, le référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information fixe les règles que doivent respecter les prestataires tiers qui réalisent des audits de la sécurité des systèmes d'information des structures. Le RGS-BF prévoit aussi des recommandations à l'intention des commanditaires d'audits, dans le cadre de la passation de marchés publics ou d'un accord contractuel, ainsi qu'aux prestataires d'audit dans le cadre de leur devoir de conseil.

Afin de s'assurer qu'elles recourent à des prestataires qui respectent ces exigences, les structures doivent, autant que possible, faire appel à des prestataires ayant obtenu une qualification, selon le schéma décrit à la section 5.

7.2.9 Réaliser une veille sur les menaces et les vulnérabilités

Se tenir informé sur l'évolution des menaces et des vulnérabilités, en identifiant les incidents qu'elles favorisent ainsi que leurs impacts potentiels, constitue une mesure fondamentale de défense. Les sites institutionnels ou ceux des éditeurs de logiciels et de matériels constituent des sources d'information essentielles sur les vulnérabilités identifiées, ainsi que sur les contre-mesures et les correctifs éventuels. Les mises à jour des logiciels et d'autres équipements, les correctifs des systèmes d'exploitation et des applications font l'objet d'alertes et d'avis qu'il est indispensable de suivre.

7.2.10 Favoriser l'interopérabilité

L'administration électronique ne saurait évoluer sans une prise en compte des règles relatives à l'interopérabilité et à la mise en cohérence des différents systèmes d'information des structures et de leurs partenaires (usagers, acteurs industriels, etc.). L'interopérabilité est en particulier traitée à travers le Référentiel général d'interopérabilité.

ANNEXE 1 GRE-1 : EXIGENCES RELATIVES AU PROCESSUS DE GESTION DES RISQUES DE SECURITE

Identification	Correspondance
ID.AM-1: Les équipements physiques sont inventoriés	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
ID.AM-2: Les plateformes logicielles et les applications sont inventoriées	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
ID.AM-3: Les flux et les processus sont formalisés et communiqués	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
ID.AM-4: Les flux d'information externes sont catalogués	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
ID.AM-5: Les ressources sont classifiées sur la base de leur criticité et de leur valeur	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
ID.AM-6: Les rôles et les responsabilités des différents intervenants (exemple : fournisseurs, clients, partenaires) sont établis	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-1: Le rôle de l'organisation dans la chaîne de valeur est identifié et communiqué	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 · NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-2: La place de l'organisation dans l'infrastructure sensible/critique est identifiée et communiquée	· COBIT 5 APO02.06, APO03.01 · NIST SP 800-53 Rev. 4 PM-8

Identification	Correspondance
ID.BE-3: Les priorités des missions organisationnelles et des objectifs sont identifiés et communiqués	· COBIT 5 APO02.01, APO02.06, APO03.01 · ISA 62443-2-1 :2009 4.2.2.1, 4.2.3.6 · NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-4: Les dépendances des services sensibles/critiques des fonctions de base sont établies et communiquées	· ISO/IEC 27001 :2013 A.11.2.2, A.11.2.3, A.12.1.3 · NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Les exigences de résilience sont établies et communiquées	· COBIT 5 DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
ID.GV-1: La politique de sécurité organisationnelle est établie	· COBIT 5 APO01.03, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls from all families
ID.GV-2: Les rôles et les responsabilités de sécurité sont établis et communiqués	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7
ID.GV-3: Les exigences réglementaires concernant la cybersécurité sont assimilées et appliquées	· COBIT 5 MEA03.01, MEA03.04 · ISA 62443-2-1:2009 4.4.3.7 · ISO/IEC 27001:2013 A.18.1 · NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
ID.GV-4: Les processus de gestion des risques sont mis en œuvre	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · NIST SP 800-53 Rev. 4 PM-9, PM-11
ID.RA-1: Les vulnérabilités sont identifiées et documentées	· CCS CSC 4 · COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1 :2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001 :2013 A.12.6.1, A.18.2.3 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Des informations à propos des menaces et des vulnérabilités sont reçues et échangées avec des parties tierces	· ISA 62443-2-1 :2009 4.2.3, 4.2.3.9, 4.2.3.12 · ISO/IEC 27001 :2013 A.6.1.4

Identification	Correspondance
	· NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5
ID.RA-3: Les menaces (externes et internes) sont identifiées et documentées	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1 :2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
ID.RA-4: Les impacts sont identifiés et documentés	· COBIT 5 DSS04.02 · ISA 62443-2-1 :2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
ID.RA-5: Les risques sont évalués sur la base des impacts, des fréquences et des classifications des ressources	· COBIT 5 APO12.02 · ISO/IEC 27001 :2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
ID.RA-6: Les solutions de sécurité sont identifiées et documentées	· COBIT 5 APO12.05, APO13.02 · NIST SP 800-53 Rev. 4 PM-4, PM-9
ID.RM-1: Des processus de gestion des risques sont mis en œuvre et validés par les parties prenantes	· COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · ISA 62443-2-1:2009 4.3.4.2 · NIST SP 800-53 Rev. 4 PM-9
ID.RM-2: La tolérance aux risques est déterminée et communiquée	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.2.6.5 · NIST SP 800-53 Rev. 4 PM-9
ID.RM-3: La tolérance aux risques est évaluée selon la sensibilité et la criticité des processus du service	· NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14

Protection	Correspondance
PR.AC-1: Les identités et les éléments d'authentification sont gérés pour les utilisateurs des systèmes sensibles	· CCS CSC 16 · COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-2, IA Family
PR.AC-2: L'accès physique aux systèmes sensibles est protégé	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
PR.AC-3: L'accès distant est contrôlé	· COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISA 62443-3-3:2013 SR 1.13, SR 2.6 · ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
PR.AC-4: Les droits d'accès sont gérés selon les principes de segregation of duties et de dual auhtorization	· CCS CSC 12, 15 · ISA 62443-2-1:2009 4.3.3.7.3 · ISA 62443-3-3:2013 SR 2.1 · ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16
PR.AC-5: L'intégrité des réseaux est protégée en utilisant la séparation physique quand nécessaire	· ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, SC-7
PR.AT-1: Les utilisateurs sont sensibilisés et formés	· CCS CSC 9 · COBIT 5 APO07.03, BAI05.07 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13
PR.AT-2: Les utilisateurs à privilège comprennent leurs rôles et responsabilités	· CCS CSC 9 · COBIT 5 APO07.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3

Protection	Correspondance
	· ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 AT-3, PM-13
PR.AT-3: Les parties prenantes tierces comprennent leurs rôles et responsabilités	· CCS CSC 9 · COBIT 5 APO07.03, APO10.04, APO10.05 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 PS-7, SA-9
PR.AT-4: Les preneurs de décision comprennent leurs rôles et responsabilités	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
PR.AT-5: Les équipes de sécurité comprennent leurs rôles et responsabilités	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
PR.DS-1: Les données stockées sont protégées	· CCS CSC 17 · COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 · ISA 62443-3-3:2013 SR 3.4, SR 4.1 · ISO/IEC 27001:2013 A.8.2.3 · NIST SP 800-53 Rev. 4 SC-28
PR.DS-2: Les données communiquées sont protégées	· CCS CSC 17 · COBIT 5 APO01.06, DSS06.06 · ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SC-8
PR.DS-3: La suppression, la déclassification et la destruction des ressources sont formalisées	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 · NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
PR.DS-4: Les moyens d'assurer la disponibilité sont définis	· COBIT 5 APO13.01 · ISA 62443-3-3:2013 SR 7.1, SR 7.2

Protection	Correspondance
	· ISO/IEC 27001:2013 A.12.3.1 · NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
PR.DS-5: La protection contre la divulgation est mise en place	· CCS CSC 17 · COBIT 5 APO01.06 · ISA 62443-3-3:2013 SR 5.2 · ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PR.DS-6: Les mécanismes de contrôle d'intégrité sont utilisés	· ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 · ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SI-7
PR.DS-7: Les environnements de développement et de test sont séparés	· COBIT 5 BAI07.04 · ISO/IEC 27001:2013 A.12.1.4 · NIST SP 800-53 Rev. 4 CM-2
PR.IP-1: Une configuration de base des systèmes et des applications est définie et maintenue	· CCS CSC 3, 10 · COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
PR.IP-2: Un cycle de vie de développement est défini	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.3 · ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
PR.IP-3: Des processus de gestion des changements de configuration sont définis	· COBIT 5 BAI06.01, BAI01.06 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10

Protection	Correspondance
PR.IP-4: Les backups sont réalisés et testés périodiquement	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.9 · ISA 62443-3-3:2013 SR 7.3, SR 7.4 · ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
PR.IP-5: Les politiques et les réglementations en matière de sécurité physique sont respectées	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
PR.IP-6: Les données sont détruites conformément à des procédures	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.4.4.4 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · NIST SP 800-53 Rev. 4 MP-6
PR.IP-7: Les processus de protection sont améliorés d'une manière continue	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
PR.IP-8: L'efficacité des mécanismes de protection est évaluée et partagée	· ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
PR.IP-9: Le BCP et DRP sont établis	· COBIT 5 DSS04.03 · ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 · NIST SP 800-53 Rev. 4 CP-2, IR-8
PR.IP-10: Les plans de réponse et de restauration sont testés	· ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.17.1.3 · NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14
PR.IP-11: La cybersécurité est considérée dans la gestion des ressources humaines	· COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4

Protection	Correspondance
	· NIST SP 800-53 Rev. 4 PS Family
PR.IP-12: Un plan de gestion des vulnérabilités est mis en œuvre	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 · NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
PR.MA-1: La maintenance et la réparation des ressources obéissent à des règles de sécurité	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.3.3.7 · ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 · NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
PR.MA-2: La maintenance à distance des ressources est contrôlée et journalisée	· COBIT 5 DSS05.04 · ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 · NIST SP 800-53 Rev. 4 MA-4
PR.PT-1: La journalisation des actions se fait conformément à des politiques	· CCS CSC 14 · COBIT 5 APO11.04 · ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · NIST SP 800-53 Rev. 4 AU Family
PR.PT-2: L'usage des supports amovibles est restreint selon des règle de sécurité	· COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 2.3 · ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7
PR.PT-3: L'accès aux systèmes est contrôlé selon le principe de least functionality	· COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · ISO/IEC 27001:2013 A.9.1.2 · NIST SP 800-53 Rev. 4 AC-3, CM-7
PR.PT-4: Les réseaux de communication et de contrôle sont protégés	· CCS CSC 7

Protection	Correspondance
	· COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7

Détection	Correspondance
DE.AE-1: Une configuration de base des performances des réseaux est définie	· COBIT 5 DSS03.01 · ISA 62443-2-1:2009 4.4.3.3 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
DE.AE-2: Les événements détectés sont analysés	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
DE.AE-3: Les événements détectés sont corrélés et agrégés pour considérer plusieurs sources	· ISA 62443-3-3:2013 SR 6.1 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DE.AE-4: L'impact des événements détectés est calculé	· COBIT 5 APO12.06 · NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4
DE.AE-5: Des seuils d'alerte sont établis	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.2.3.10 · NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
DE.CM-1: Les réseaux sont surveillés pour la détection des incidents de cybersécurité	· CCS CSC 14, 16 · COBIT 5 DSS05.07 · ISA 62443-3-3:2013 SR 6.2 · NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DE.CM-2: L'environnement physique est contrôlé pour la détection des incidents de cybersécurité	· ISA 62443-2-1:2009 4.3.3.3.8 · NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
DE.CM-3: L'activité du personnel est surveillée pour la détection des incidents de cybersécurité	· ISA 62443-3-3:2013 SR 6.2 · ISO/IEC 27001:2013 A.12.4.1 · NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11

Détection	Correspondance
DE.CM-4: Les codes malveillants sont détectés	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.3.4.3.8 · ISA 62443-3-3:2013 SR 3.2 · ISO/IEC 27001:2013 A.12.2.1 · NIST SP 800-53 Rev. 4 SI-3
DE.CM-5: Les codes mobiles non autorisés sont détectés	· ISA 62443-3-3:2013 SR 2.4 · ISO/IEC 27001:2013 A.12.5.1 · NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
DE.CM-6: Les activités des fournisseurs de services externes sont surveillées pour la détection des événements de cybersécurité	· COBIT 5 APO07.06 · ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 · NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Les accès non-autorisés sont surveillés	· NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DE.CM-8: Des scans de vulnérabilité sont réalisés périodiquement	· COBIT 5 BAI03.10 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-5
DE.DP-1: Les rôles et les responsabilités du processus de détection des incidents sont définis	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.4.3.1 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
DE.DP-2: Les exigences de détection sont définies et appliquées	· ISA 62443-2-1:2009 4.4.3.2 · ISO/IEC 27001:2013 A.18.1.4 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
DE.DP-3: Les processus de détection sont testés	· COBIT 5 APO13.02 · ISA 62443-2-1:2009 4.4.3.2 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.14.2.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
DE.DP-4: Les événements détectés sont communiqués	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.4.5.9 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4

Détection	Correspondance
DE.DP-5: Le processus de détection fait l'objet d'une amélioration continue	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Réponse	Correspondance
RS.RP-1: Les plans de réponse sont déclenchés lors de l'occurrence d'un incident	· COBIT 5 BAI01.10 · CCS CSC 18 · ISA 62443-2-1 :2009 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
RS.CO-1: Le personnel est avisé de l'ordre des opérations de réponse	· ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 · NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
RS.CO-2: Les événements sont reportés en conformité avec les exigences de sécurité	· ISA 62443-2-1:2009 4.3.4.5.5 · ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
RS.CO-3: L'information est partagée conformément au plan de réponse	· ISA 62443-2-1 :2009 4.3.4.5.2 · ISO/IEC 27001 :2013 A.16.1.2 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RS.CO-4: La coordination avec les parties prenantes se fait conformément au processus de réponse	· ISA 62443-2-1:2009 4.3.4.5.5 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RS.CO-5: Le partage volontaire d'information se fait en conformité avec le plan de réponse	· NIST SP 800-53 Rev. 4 PM-15, SI-5
RS.AN-1: Les notifications d'événements font preuve d'investigation	· COBIT 5 DSS02.07 · ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2: L'impact d'un incident est déterminé suite à une enquête	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISO/IEC 27001:2013 A.16.1.6

Réponse	Correspondance
	· NIST SP 800-53 Rev. 4 CP-2, IR-4
RS.AN-3: Des processus d'investigation numériques sont réalisés en cas de l'occurrence d'un incident	· ISA 62443-3-3 :2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · ISO/IEC 27001 :2013 A.16.1.7 · NIST SP 800-53 Rev. 4 AU-7, IR-4
RS.AN-4: Les incidents sont classés selon le plan de réponse	· ISA 62443-2-1:2009 4.3.4.5.6 · ISO/IEC 27001:2013 A.16.1.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
RS.MI-1: Le confinement des incidents est réalisé conformément au plan de réponse	· ISA 62443-2-1:2009 4.3.4.5.6 · ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
RS.MI-2: Les incidents sont contrôlés selon le plan de réponse	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 · ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4
RS.MI-3: Les vulnérabilités nouvellement détectées sont répertoriées comme des risques acceptés	· ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
RS.IM-1: Les leçons des incidents précédents sont formellement classées	· COBIT 5 BAI01.13 · ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RS.IM-2: Un processus de révision du plan de réponse est mis en œuvre	· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

Restauration	Correspondance
RC.RP-1: Le plan de restauration est déclenché en cas d'occurrence d'un incident de sécurité	· CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
RC.IM-1: Les leçons acquises lors du déclenchement du plan de restauration sont formellement classées	· COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RC.IM-2: Les stratégies de restauration sont mises à jour	· COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RC.CO-1: Les relations publiques sont gérées lors de l'exécution du plan de restauration	· COBIT 5 EDM03.02
RC.CO-2: La réputation fait partie des critères du processus de restauration	· COBIT 5 MEA03.02
RC.CO-3: Les activités de restauration sont communiquées aux parties concernées	· NIST SP 800-53 Rev. 4 CP-2, IR-4

ANNEXE 2 GRE-2 : EXIGENCES RELATIVES A L'ANALYSE DES RISQUES DE SECURITE DANS UN CONTEXTE INTERNE

GRE-2-1 : Détermination de l'échelle des fréquences

Les valeurs **F1**, **F2**, **F3**, **F4** et **F5** doivent être définies par l'entité bénéficiaire (faisant partie du périmètre RGS-BF) pour chaque mission d'analyse des risques. Elles consistent en un chiffre qui traduit les chances d'occurrence de la menace pendant une année.

Exemples :

- Pour un cas de figure où il est estimé que la fréquence pour l'échelle **C** est de 3 fois par an, la valeur sera **F3** = 3.
- Pour un cas de figure où il est estimé que la fréquence pour l'échelle **A** est de 1 fois tous les 5 ans, la valeur sera **F1**=0.2.

Tableau 2: Echelle de fréquences.

Fréquence					
Echelle	**A**	**B**	**C**	**D**	**E**
Label	Rare	Peu probable	Probable	Très probable	~certain
Valeur	**F1**	**F2**	**F3**	**F4**	**F5**
Description	Peut survenir dans des circonstances exceptionnelles	Peut survenir parfois dans certaines circonstances	Survient parfois dans certaines circonstances	Survient probablement dans la plupart des circonstances	Survient certainement dans la plupart des circonstances

GRE-2-2 : Détermination de l'échelle des impacts

La description des niveaux d'impact **faible**, **moyen** et **haut** est donnée dans le Tableau 3. Les valeurs **I1**, **I2** et **I3** seront définies par la structure pour chaque mission d'analyse des risques. Elles consistent en un chiffre qui traduit les dégâts financiers engendrés par une occurrence de la menace considérée.

Tableau 3: Echelle d'impact.

Impact			
Echelle	1	2	3
Label	Bas	Moyen	Haut
Objectif de sécurité	Description		
Confidentialité/Intégrité/Disponibilité	La non-atteinte de l'objectif engendre : • une perte financière négligeable (**I1**) • une dégradation dans la conduite de certains processus, mais pas un arrêt des missions principales • des dégâts mineurs sur les ressources organisationnelles	La non-atteinte de l'objectif engendre • une perte financière significative (**I2**) • une dégradation significative dans la conduite de certains processus, mais pas un arrêt des missions principales • des dégâts significatifs sur les ressources organisationnelles	La non-atteinte de l'objectif engendre • une perte financière très importante (**I3**) • une dégradation très importante dans la conduite de certains processus, et l'arrêt de certaines missions principales • des dégâts très importants sur les ressources organisationnelles

ANNEXE 3 GRE-3 : EXIGENCES RELATIVES A L'ANALYSE DES RISQUES DE SECURITE DANS LE CONTEXTE NATIONAL

Identification
ID.AM-1: Les équipements physiques sont inventoriés
ID.AM-2: Les plateformes logicielles et les applications sont inventoriées
ID.AM-3: Les flux et les processus sont formalisés et communiqués
ID.AM-4: Les flux d'information externes sont catalogués
ID.AM-5: Les ressources sont classifiées sur la base de leur criticité et de leur valeur
ID.AM-6: Les rôles et les responsabilités des différents intervenants (exemple : fournisseurs, clients, partenaires) sont établis
ID.BE-1: Le rôle de l'organisation dans la chaîne de valeur est identifié et communiqué
ID.BE-2: La place de l'organisation dans l'infrastructure sensible/critique est identifiée et communiquée
ID.BE-3: Les priorités des missions organisationnelles et des objectifs sont identifiés et communiqués
ID.BE-4: Les dépendances des services sensibles/critiques des fonctions de base sont établies et communiquées
ID.BE-5: Les exigences de résilience sont établies et communiquées
ID.GV-1: La politique de sécurité organisationnelle est établie
ID.GV-2: Les rôles et les responsabilités de sécurité sont établis et communiqués
ID.GV-3: Les exigences réglementaires concernant la cybersécurité sont assimilées et appliquées
ID.GV-4: Les processus de gestion de risque sont mis en œuvre
ID.RA-1: Les vulnérabilités sont identifiées et documentées
ID.RA-2: Des informations à propos des menaces et des vulnérabilités sont reçues et échangées avec des parties tierces
ID.RA-3: Les menaces (externes et internes) sont identifiées et documentées
ID.RA-4: Les impacts sont identifiés et documentés
ID.RA-5: Les risques sont évalués sur la base des impacts, des fréquences et des classifications des ressources
ID.RA-6: Les solutions de sécurité sont identifiées et documentées
ID.RM-1: Des processus de gestion des risques sont mis en œuvre et validés par les parties prenantes
ID.RM-2: La tolérance aux risques est déterminée et communiquée
ID.RM-3: La tolérance aux risques et évaluée selon la sensibilité et la criticité des processus du service
Protection
PR.AC-1: Les identités et les éléments d'authentification sont gérés pour les utilisateurs des systèmes sensibles
PR.AC-2: L'accès physique aux systèmes sensibles est protégé
PR.AC-3: L'accès distant est contrôlé

PR.AC-4: Les droits d'accès sont gérés selon les principes de segregation of duties et de dual auhtorization
PR.AC-5: L'intégrité des réseaux est protégée en utilisant la séparation physique quand nécessaire
PR.AT-1: Les utilisateurs sont sensibilisés et formés
PR.AT-2: Les utilisateurs à privilège comprennent leurs rôles et responsabilités
PR.AT-3: Les parties prenantes tierces comprennent leurs rôles et responsabilités
PR.AT-4: Les preneurs de décision comprennent leurs rôles et responsabilités
PR.AT-5: Les équipes de sécurité comprennent leurs rôles et responsabilités
PR.DS-1: Les données stockées sont protégées
PR.DS-2: Les données communiquées sont protégées
PR.DS-3: La suppression, la déclassification et la destruction des ressources sont formalisées
PR.DS-4: Les moyens d'assurer la disponibilité sont définis
PR.DS-5: La protection contre la divulgation est mise en place
PR.DS-6: Les mécanismes de contrôle d'intégrité sont utilisés
PR.DS-7: Les environnements de développement et de test sont séparés
PR.IP-1: Une configuration de base des systèmes et des applications est définie et maintenue
PR.IP-2: Un cycle de vie de développement est défini
PR.IP-3: Des processus de gestion des changements de configuration sont définis
PR.IP-4: Les backups sont réalisés et testés périodiquement
PR.IP-5: Les politiques et les réglementations en matière de sécurité physique sont respectées
PR.IP-6: Les données sont détruites conformément à des procédures
PR.IP-7: Les processus de protection sont améliorés d'une manière continue
PR.IP-8: L'efficacité des mécanismes de protection est évaluée et partagée
PR.IP-9: Le BCP et DRP sont établis
PR.IP-10: Les plans de réponse et de restauration sont testés
PR.IP-11: La cybersécurité est considérée dans la gestion des ressources humaines
PR.IP-12: Un plan de gestion des vulnérabilités est mis en œuvre
PR.MA-1: La maintenance et la réparation des ressources obéit à des règles de sécurité
PR.MA-2: La maintenance à distance des ressources est contrôlée et journalisée
PR.PT-1: La journalisation des actions se fait conformément à des politiques
PR.PT-2: L'usage des supports amovibles est restreint selon des règles de sécurité
PR.PT-3: L'accès aux systèmes est contrôlé selon le principe de least functionality
PR.PT-4: Les réseaux de communication et de contrôle sont protégés

Détection
DE.AE-1: Une configuration de base des performances des réseaux est définie
DE.AE-2: Les événements détectés sont analysés
DE.AE-3: Les événements détectés sont corrélés et agrégés pour considérer plusieurs sources
DE.AE-4: L'impact des événements détectés est calculé
DE.AE-5: Des seuils d'alerte sont établis
DE.CM-1: Les réseaux sont surveillés pour la détection des incidents de cybersécurité
DE.CM-2: L'environnement physique est contrôlé pour la détection des incidents de cybersécurité
DE.CM-3: L'activité du personnel est surveillée pour la détection des incidents de cybersécurité
DE.CM-4: Les codes malveillants sont détectés
DE.CM-5: Les codes mobiles non autorisés sont détectés
DE.CM-6: Les activités des fournisseurs de services externes sont surveillées pour la détection des événements de cybersécurité
DE.CM-7: Les accès non-autorisés sont surveillés
DE.CM-8: Des scans de vulnérabilité sont réalisés périodiquement
DE.DP-1: Les rôles et les responsabilités du processus de détection des incidents sont définis
DE.DP-2: Les exigences de détection sont définies et appliquées
DE.DP-3: Les processus de détection sont testés
DE.DP-4: Les événements détectés sont communiqués
DE.DP-5: Le processus de détection fait l'objet d'une amélioration continue

Réponse
RS.RP-1: Les plans de réponse sont déclenchés lors de l'occurrence d'un incident
RS.CO-1: Le personnel est avisé de l'ordre des opérations de réponse
RS.CO-2: Les événements sont reportés en conformité avec les exigences de sécurité
RS.CO-3: L'information est partagée conformément au plan de réponse
RS.CO-4: La coordination avec les parties prenantes se fait conformément au processus de réponse
RS.CO-5: Le partage volontaire d'information se fait en conformité avec le plan de réponse
RS.AN-1: Les notifications d'événements font preuve d'investigation
RS.AN-2: L'impact d'un incident est déterminé suite à une enquête
RS.AN-3: Des processus d'investigation numériques sont réalisés en cas de l'occurrence d'un incident
RS.AN-4: Les incidents sont classés selon le plan de réponse
RS.MI-1: Le confinement des incidents est réalisé conformément au plan de réponse
RS.MI-2: Les incidents sont contrôlés selon le plan de réponse
RS.MI-3: Les vulnérabilités nouvellement détectées sont répertoriées comme des risques acceptés
RS.IM-1: Les leçons des incidents précédents sont formellement classées
RS.IM-2: Un processus de révision du plan de réponse est mis en œuvre

Restauration
RC.RP-1: Le plan de restauration est déclenché en cas d'occurrence d'un incident de sécurité
RC.IM-1: Les leçons acquises lors du déclenchement du plan de restauration sont formellement classées
RC.IM-2: Les stratégies de restauration sont mises à jour
RC.CO-1: Les relations publiques sont gérées lors de l'exécution du plan de restauration
RC.CO-2: La réputation fait partie des critères du processus de restauration
RC.CO-3: Les activités de restauration sont communiquées aux parties concernées

ANNEXE 4 STE-1 : EXIGENCES RELATIVES A LA CRYPTOLOGIE

STE-1-1 Catégories d'algorithmes cryptographiques

- **Algorithmes de cryptage symétrique** : Ce sont des algorithmes où le cryptage et le décryptage se font par la même clé secrète. Cette clé doit être partagée entre l'émetteur et le récepteur par un mécanisme sécurisé. Il existe deux (02) types de cryptage symétrique : le cryptage par bloc et le cryptage par flux. Le premier crypte le texte clair en opérant sur des blocs de taille fixe. Le deuxième réalise le cryptage bit par bit. On recommande les algorithmes de cryptage symétrique par bloc.
- **Algorithmes de cryptage asymétrique** : Ce sont des algorithmes qui utilisent une paire de clés (publique, privée) associées de sorte qu'un message crypté (resp. signé) par la clé publique (resp. privée) ne peut être décrypté (resp. vérifié) que par la clé privée (resp. publique) associée. Ces algorithmes ne requièrent pas un mécanisme de partage de clés puisque la clé publique peut être connue publiquement alors que la clé privée ne doit jamais être transmise ou partagée. Etant plus lents que les algorithmes symétriques, les algorithmes asymétriques sont généralement utilisés pour l'établissement de la clé secrète d'un algorithme symétrique ou encore pour les signatures numériques.
- **Fonctions de hachage** : Ce sont des fonctions à sens unique (irréversibles) qui permettent de produire à partir d'un message quelconque un condensé unique de taille fixe. Ce condensé ne donne aucun renseignement sur le message initial grâce à l'irréversibilité de la fonction de hachage, et à l'absence de collision. En effet deux (02) messages distincts ne donneront théoriquement jamais un même condensé. Les fonctions de hachage assurent l'intégrité des messages hachés.

STE-1-2 AES : Advanced Encryption Standard

Advanced Encryption Standard (AES) est un algorithme de cryptage symétrique par bloc qui s'applique à des blocs de 128 bits en utilisant des clés de tailles 128 bits, 196 bits ou 256 bits. L'algorithme réalise un ensemble de tours composés de quatre (04) transformations (réversibles) chacun (sauf le dernier tour : trois (03) transformations). Les détails de l'algorithme sont publiés dans le standard AES FIPS PUB 197.

STE-1-3 Cryptage asymétrique

Le cryptage asymétrique repose la difficulté pour un attaquant de résoudre certains problèmes mathématiques à savoir le problème de factorisation, le problème du logarithme discret dans les corps finis, et le problème du logarithme discret dans le corps des courbes elliptiques. Ces problèmes sont formulés dans ce qui suit :

- **Problème de factorisation** : Etant donné un entier n suffisamment grand, trouver deux (02) nombre premiers p et q tels que n soit le produit de p et q.
- **Problème du logarithme discret dans les corps finis** : étant donné un groupe cyclique multiplicatif G d'ordre n et de générateur g, et un élément y du groupe, trouver le plus petit élément x du groupe G tel que y soit égal au générateur g puissance x.
- **Problème du logarithme discret dans les corps de courbes elliptiques :** étant donné une courbe elliptique E définie sur un corps fini F, et deux (02) points A et B de la courbe, trouver un entier d de F tel que A soit le résultat de la multiplication scalaire de B par d (dans le corps des points de la courbes elliptique cette multiplication scalaire consiste à additionner B à lui-même d fois).

Parmi les algorithmes qui se basent sur ces problèmes, RSA et ECDSA sont recommandés comme algorithmes asymétriques.

1 RSA

- RSA est un algorithme de cryptage asymétrique basé sur un module, un exposant publique et un exposant secret. L'opération de cryptage qui donne la confidentialité consiste à élever le texte clair à la puissance l'exposant public alors que l'intégrité et l'authentification sont données par le fait d'élever le texte chiffré à la puissance l'exposant secret. La robustesse de RSA est basée sur la difficulté de factoriser le module en produit de deux (02) nombres premiers. L'algorithme est publié dans le standard PKCS#1 :RSA Cryptography Standard.

2 ECDSA

- ECDSA est un algorithme de signature numérique opérant dans le corps des points d'une courbe elliptique. Après avoir fait le hachage du texte à signer, on tronque un nombre de bit de poids le plus fort de même taille que l'ordre du groupe dans lequel est définie la courbe elliptique. La clé privée utilisée pour signer est un nombre strictement inférieur à l'ordre du groupe choisi aléatoirement en respectant des conditions. La clé publique est la multiplication scalaire de la clé privée avec le point générateur de la courbe elliptique. Les processus de signature et de vérification assurent l'intégrité du texte signé, l'authentification du signataire et la non répudiation de la signature par ce dernier. Ces processus sont détaillés dans le standard DSS FIPS PUB 186-4.

STE-1-4 Fonctions de hachage

- Les fonctions de hachage recommandées appartiennent à la famille SHA-2, avec des condensés de tailles 256, 384 et 512 bits. Les algorithmes SHA-256 et SHA-512 utilisent des mots de taille 32 et 64 bits respectivement. L'algorithme SHA-384 est une

version tronquée de SHA-512. Opérant très semblablement, les principales différences entres SHA-256 et SHA-512 résident dans les quantités de décalage et les constantes additives. Ces fonctions sont détaillées dans le standard FIPS PUB 180-4.

STE-1-5 Cas d'usages des clés

Type de clé	Usage
Clé privée de signature	Assure l'authentification de la source, l'intégrité et la non répudiation lors de la signature par un algorithme asymétrique de signature numérique.
Clé publique de signature	Assure l'authentification de la source, l'intégrité et la non répudiation lors de la vérification de la signature par un algorithme asymétrique de signature numérique.
Clé symétrique d'authentification	Assure l'authentification de la source et l'intégrité dans les algorithmes de cryptage symétrique. En cas de cryptage authentifié, la même clé est utilisée pour l'authentification et pour le cryptage.
Clé privée d'authentification	Assure l'authentification de la source dans les algorithmes de cryptage asymétrique lors de l'établissement d'une session de communication authentifiée.
Clé publique d'authentification	Assure l'authentification de la source dans les algorithmes de cryptage asymétrique lors de l'établissement d'une session de communication authentifiée.
Clé symétrique de cryptage de données	Assure la confidentialité (par le cryptage) des données dans les algorithmes de cryptage symétriques. La même clé est utilisée pour le décryptage.
Clé symétrique de cryptage de clé	Clé utilisée pour crypter d'autres clés avec des algorithmes de cryptage symétriques. La même clé est aussi utilisée pour décrypter la clé cryptée. Dans certains cas, elle assure aussi l'intégrité.
Clés symétriques pour RBG	Clés utilisées pour générer des nombres ou des bits aléatoires.
Clé maître symétrique	Clé utilisée pour dériver d'autres clés (de cryptage de données ou de cryptage de clés) avec des méthodes de cryptage symétriques

Type de clé	Usage
Clé privée pour le transport de clé	Clé utilisée pour décrypter des clés qui ont été préalablement cryptées par la clé publique correspondante avec un algorithme de cryptage asymétrique. Ces clés sont utilisées pour l'établissement de clés (clés de cryptage de clés ou de données, vecteurs d'initialisation).
Clé publique pour le transport de clé	Clé publique utilisée pour crypter des clés avec un algorithme de cryptage asymétrique. Ces clés sont utilisées pour l'établissement de clés (clés de cryptage de clés ou de données, vecteurs d'initialisation).
Clé symétrique pour l'échange de clé	Clé utilisée pour l'établissement de clés (clés de cryptage de clés ou de données, vecteurs d'initialisation) avec un algorithme de cryptage symétrique.
Clé privée pour l'échange de clé	Clé privée utilisée pour l'établissement de clés (clés de cryptage de clés ou de données, vecteurs d'initialisation) à long terme avec un algorithme de cryptage asymétrique.
Clé publique pour l'échange de clé	Clé publique utilisée pour l'établissement de clés (clés de cryptage de clés ou de données, vecteurs d'initialisation) à long terme avec un algorithme de cryptage asymétrique.
Clé privée unique pour l'échange de clé	Clé privée utilisée une seule fois pour l'établissement d'une ou plusieurs clés (clés de cryptage de clés ou de données, vecteurs d'initialisation) avec un algorithme de cryptage asymétrique.
Clé publique unique pour l'échange de clé	Clé publique utilisée une seule fois pour l'établissement d'une ou plusieurs clés (clés de cryptage de clés ou de données, vecteurs d'initialisation) avec un algorithme de cryptage asymétrique.
Clé symétrique d'autorisation	Clé utilisée pour donner des privilèges à une entité en utilisant une méthode de cryptage symétrique. Cette clé est connue de l'entité responsable de donner les privilèges et l'entité demandant les privilèges d'accès.
Clé privée d'autorisation	Clé privée d'une paire de clés asymétriques utilisée pour donner des privilèges à une entité.

Type de clé	Usage
Clé publique d'autorisation	Clé publique d'une paire de clés asymétriques utilisée pour donner des privilèges à une entité.

STE-1-6 : Robustesse par rapport à la cryptanalyse

Type de clé	Cryptopériode	
	Période pour l'usage de l'initiateur (OUP)	Période pour l'usage du récepteur
Clé privée de signature	1-3 années	
Clé publique de signature	Plusieurs années (dépendant de la taille de la clé)	
Clé symétrique d'authentification	<= 2 années	<= OUP + 3 années
Clé privée d'authentification	1-2 années	
Clé publique d'authentification	1-2 années	
Clé symétrique de chiffrement de données	<= 2 années	<= OUP + 3 années
Clé symétrique de chiffrement de clé	<= 2 années	<= OUP + 3 années
Clés symétriques pour RBG	Déterminée par conception	
Clé maître symétrique	Environ 1 an	
Clé privée pour le transport de clé	<= 2 années	
Clé publique pour le transport de clé	1-2 années	
Clé symétrique pour l'échange de clé	1-2 années	
Clé privée pour l'échange de clé	1-2 années	
Clé publique pour l'échange de clé	1-2 années	
Clé privée unique pour l'échange de clé	Une clé unique par transaction	
Clé publique unique pour l'échange de clé	Une clé unique par transaction	

Type de clé	Cryptopériode	
	Période pour l'usage de l'initiateur (OUP)	Période pour l'usage du récepteur
Clé symétrique d'autorisation	<= 2 années	
Clé privée d'autorisation	<= 2 années	
Clé publique d'autorisation	<= 2 années	

Date	Résistance minimale	Algorithme symétrique	Factorisation Module	Logarithme discret		Courbe elliptique	Hash (A)	Hash (B)
				Clé	Groupe			
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 et au-delà	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 et au-delà	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 et au-delà	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

ANNEXE 5 STE-2 : EXIGENCES RELATIVES A L'ACCREDITATION DES PRESTATAIRES DE SERVICES DE CONFIANCE

STE-2-1 : Procédure d'accréditation

Les étapes de ce processus sont :

1. Soumission du dossier : consiste à soumettre une demande d'accréditation en vue d'avoir le statut de prestataire de service de confiance. Cette demande est constituée des pièces suivantes :
    - Identification du prestataire : nom et prénom pour les personnes physiques et raison sociale pour les personnes morales.
    - Adresse : indication précise de l'adresse de(s) l'établissement(s) où seront hébergés les services de certification faisant l'objet de la demande d'accréditation.
    - Ressources humaines : liste complète des ressources humaines qui seront impliqués dans l'activité qui fait l'objet de l'accréditation.
    - Ressources techniques : description des dispositifs techniques qui seront mis en place pour l'activité qui fait l'objet de l'accréditation ainsi qu'une copie de tous certificats de conformité du dispositif établi par d'autres organismes d'évaluation régionaux ou internationaux.
    - Documentation : politique de certification, politique de sécurité, statut de l'entreprise…
    - Identification du service requis : indication du ou des service(s) (parmi ceux définis dans l'Article 80 de la Loi 045/2009) pour lesquels la demande d'accréditation est présentée.
2. Vérification de la complétude du dossier : le dossier doit obligatoirement comporter la totalité des pièces mentionnées dans le point précédent. Autrement, la demande est rejetée sans passer aux autres étapes du processus. Une notification est préparée à cet effet et est remise au demandeur.
3. Analyse de la documentation : au niveau de cette étape, une revue des politiques, procédures et instructions, tant au plan organisationnel que technique est élaborée.
4. Analyse technique : un ensemble de critères techniques doivent être vérifiés dans les dispositifs techniques mis en œuvre par le prestataire en vue de se voir octroyer l'accréditation. Le dispositif cryptographique permettant de procéder à la génération et la gestion des conventions secrètes doit répondre aux exigences de sécurité suivantes :

- garantir la robustesse cryptographique des conventions secrètes générées ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération, et disposer de techniques sûres de destruction des conventions secrètes qui ne sont plus utilisées ;
- garantir la confidentialité et l'intégrité des conventions secrètes ;
- assurer l'accès aux conventions secrètes exclusivement aux utilisateurs autorisés et protéger lesdites conventions contre toute utilisation par des tiers.

En outre, le dispositif cryptographique permettant le chiffrement des données à protéger doit répondre aux exigences de sécurité suivantes :

- garantir la confidentialité et l'intégrité des données à chiffrer ;
- assurer l'accès aux conventions secrètes exclusivement aux utilisateurs autorisés et protéger lesdites conventions contre toute utilisation par des tiers.

5. Notification : sur la base d'un rapport d'audit, une notification du résultat de l'instruction du dossier d'accréditation est communiquée au demandeur. En cas de refus, les raisons seront clairement mentionnées.

La loi 045/2009 stipule que la durée de la première étape est de dix (10) jours. Si le dossier soumis est complet, un reçu est délivré au demandeur (avec une indication sur la suite de la procédure), alors que, dans le cas contraire, un refus lui est délivré.

En outre, la validité de l'accréditation est de trois (03) ans et son renouvellement est conditionné par une reconduite du processus ci-dessus dans un délai ne dépassant pas trois (03) mois de l'expiration de l'accréditation courante.

À cet effet, la structure adresse à l'ARCEP un dossier de demande de validation qui documente les actions suivantes :

- rédiger une Politique de Certification (PC) conforme aux modèles définis par l'autorité d'accréditation ;
- mettre en œuvre des clés cryptographiques pour les autorités de certifications faisant partie du périmètre du PSCO. Ces clés sont spécifiquement restreintes et dédiées à la génération de certificats destinés aux autorités ou à leurs agents et mentionner cette exigence dans la PC ;

- générer des certificats à destination exclusive des autorités de certifications ou de leurs agents et mentionner explicitement cette exigence dans la PC ;
- établir des procédures avec ces prestataires permettant de garantir le respect par ces prestataires de la PC pour ce qui les concerne lorsque le PSCO recourt à des prestataires externes pour certaines fonctions.

L'ARCEP peut, à tout moment, demander de vérifier sur place les conditions de délivrance des certificats afin de s'assurer que les procédures mises en place par l'AC sont conformes au présent référentiel. En cas de non-conformité signalée par l'ANSSI, la structure dispose d'un délai de trois (03) mois pour faire corriger les procédures de l'AC. À défaut, les certificats ne sont plus considérés comme conformes au RGS-BF. L'ARCEP publie le nouveau statut de ce certificat sur son site.

L'ARCEP doit faire une demande de renouvellement de la validation lors de chaque modification substantielle des conditions de délivrance des certificats, notamment lorsque le certificat de l'AC est expiré.

STE-2-2 : Procédure d'audit et de contrôle

Les principaux points qui constituent le processus de contrôle sont discutés dans cette section.

Le prestataire doit respecter et contrôler les mesures de sécurité qu'il met en place pour le bon fonctionnement de ses activités et notamment celles qui concernent la sécurité relative au personnel employé dans la fourniture des prestations de cryptologie, aux équipements, aux informations et aux locaux utilisés, ainsi que les mesures prises en cas de gestion d'incidents en vue de prévenir les fraudes et les failles de sécurité.

Les locaux doivent être aménagés de façon à assurer la sécurité des conventions secrètes suivant les prescriptions ci-après :

- disposer d'au moins une zone à accès contrôlé, contre toute intrusion extérieure, pour abriter les activités de gestion, de mise en œuvre ou de remise des conventions secrètes. L'accès à cette zone est contrôlé par tout moyen physique et enregistré. Le personnel autorisé à y accéder est limité au strict besoin du bon fonctionnement du service et figure sur une liste établie et mise à jour à cet effet;
- renforcer la sécurité de cette zone, en dehors des heures ouvrables, par la mise en œuvre de moyens de détection d'intrusion physique ;

- communiquer à l'ARCEP la localisation de cette zone, la description des dispositifs de sécurité mis en place et la liste du personnel autorisé à y accéder;
- en cas de constatation de toute intrusion ou de toute tentative d'intrusion visant à pénétrer dans cette zone, ouvrir une enquête interne et, le cas échéant, déposer une plainte auprès de l'autorité compétente dans les vingt-quatre (24) heures qui suivent.

De plus les systèmes informatiques utilisés par le prestataire dans le cadre de ses activités ne doivent en aucun cas être utilisés à d'autres fins. Ils doivent aussi comporter les fonctionnalités suivantes :

- l'identification et l'authentification des utilisateurs des systèmes informatiques ;
- la limitation des droits d'accès au strict besoin du service. Pendant toute la durée de leur détention, les conventions secrètes sont chiffrées. Elles ne sont déchiffrées que pour être mises en œuvre ou remises ;
- l'imputabilité de toute opération permettant d'accéder aux conventions secrètes ou autres ressources de sécurité du système à son auteur ;
- l'audit au moyen d'un enregistrement, sauvegardé régulièrement et archivé, de toute opération permettant l'accès aux conventions secrètes ou aux autres ressources de sécurité du système ;
- la mise à zéro au moyen d'un dispositif, de tous les objets de stockage ayant contenu une ressource sensible du système informatique avant toute utilisation ultérieure desdits objets. Lorsqu'il n'est plus utilisé, le dispositif de mise à zéro est détruit et sa destruction fait l'objet d'un compte rendu.

Le prestataire doit disposer d'un lieu sécurisé spécialement aménagé, pour la conservation des dispositifs servant à déchiffrer les conventions secrètes et dont l'accès est réservé aux seules personnes qu'il a autorisées.

Le périmètre à accréditer doit comporter tous les éléments indispensables au fonctionnement du système. La délimitation du périmètre ne doit comporter aucune ambiguïté, car elle permet de déterminer et de caractériser précisément les systèmes qui seront homologués. La description de ce périmètre comprend :

- des éléments fonctionnels et d'organisation : fonctionnalités du système, type d'utilisateurs, contexte et règles d'emploi, procédures formalisées, conditions d'emploi des produits de sécurité, gestion des droits, dispositifs de détection et de gestion des incidents ;

- des éléments techniques : architecture du système (en précisant notamment les interconnexions avec d'autres systèmes), possibilité d'utilisation de supports amovibles, d'accès à distance ou de cloisonnement, mécanismes de maintenance, d'exploitation ou de télégestion du système, notamment lorsque ces opérations sont effectuées par des prestataires externes ;
- les ressources humaines : compétences des personnes physiques, expertise et expérience, organisation et bonnes pratiques.
- le périmètre géographique et physique : localisations géographiques et caractéristiques des locaux.

En matière d'exigences techniques, les plus importantes sont celles relatives à la protection de la clé privée. L'accréditation doit donc inclure les vérifications suivantes :

- si la paire de clés du serveur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération, et disposer de techniques sûres de destruction de la clé privée en cas de régénération de la clé privée ; garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une authentification qui ne peut être falsifiée (générée d'une manière non autorisée) sans la connaissance de la clé privée ;
- assurer pour le serveur légitime uniquement, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers ;
- permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

En outre, la protection de l'environnement obéit à un ensemble de règles. Dans les cadres d'accréditation étudiées, les exigences types suivantes ont été dégagées:

- protection contre les virus, avec mises à jour régulières ;
- contrôle et limitation des échanges entre la machine hôte et d'autres machines dans un réseau ouvert ;

- restriction, lorsque cela est possible, de l'accès aux fonctions d'administration de la machine aux seuls administrateurs de celles-ci (différenciation compte utilisateur/administrateur) ;
- installation et mise à jour de logiciels et de composants sur la machine sous le contrôle de l'administrateur ;
- refus par le système d'exploitation de l'ordinateur ou de la borne d'exécuter des applications téléchargées ne provenant pas de sources sûres ; mise à jour des composants logiciels et systèmes lors de la mise à disposition de mises à jour de sécurité de ceux-ci.

Pour se faire accréditer, le PSCO doit élaborer un référentiel documentaire. Les principales actions à réaliser dans ce cadre sont :

- rédiger une Politique de Certification (PC) conforme aux modèles définis par l'autorité d'accréditation ;
- mettre en œuvre des clés cryptographiques pour les autorités de certifications faisant partie du périmètre du PSCO. Ces clés sont spécifiquement restreintes et dédiées à la génération de certificats destinés aux autorités ou à leurs agents et mentionner cette exigence dans la PC ;
- générer des certificats à destination exclusive des autorités de certifications ou de leurs agents et mentionner explicitement cette exigence dans la PC ;
- établir des procédures avec ces prestataires permettant de garantir le respect par ces prestataires de la PC pour ce qui les concerne lorsque le PSCO recourt à des prestataires externes pour certaines fonctions.

Les principaux axes considérés dans l'accréditation des PSCOs dans le cas des pays de l'échantillon sont résumés ci-dessous :

- étude de la population/des utilisateurs à qui est destiné le certificat en tenant compte à la fois des caractéristiques des utilisateurs, de l'utilisation qui sera faite du certificat (signature, chiffrement entre entités morales et/ou physiques, accès à des applications sécurisées) et de la mise en place des critères d'attribution ;
- étude des moyens de collecte des informations, de leur validation et de la création des certificats ;
- définition de la durée de vie des clés (privée, publique et/ou de session), des certificats, de la consolidation de ceux-ci, de la gestion des listes de révocations ;
- étude des moyens de distribution des certificats via des communications sécurisées de type « VPN » ou sur un support style « carte de crédit » avec récupération en main propre ou par un agent de sécurité sur site ;

- sécurité des ICP au sens implantation physique, et sécurité des annuaires supports des informations publiques en tenant compte de l'infrastructure, de l'administration et du coût de gestion ;
- définition des services nécessitant une haute disponibilité (exemple : gestion des listes de révocation) ;
- prise en compte de la nécessité d'un recouvrement des clés privées et de l'interaction avec l'autorité suprême et/ou avec d'autres communautés (interopérabilité pour certifications croisées) ;
- étude du support matériel/logiciel du certificat chez l'utilisateur en tenant compte de la vétusté des postes de travail et en prévoyant des évolutions aisées ;
- prise en compte de l'impact sur les structures existantes : physiques et organisationnelles ;
- définition de la formation/information des acteurs impliqués dans le processus de gestion de l'infrastructure de confiance.

ANNEXE 6 STE-3 : EXIGENCES RELATIVES AUX POLITIQUES DE CERTIFICATION

STE-3-1 : Critères organisationnels

Aspects généraux

Convention de noms

Q1	Les procédures du prestataire de services de confiance garantissent-elles que, dans les certificats X.509v3, l'émetteur et le porteur sont identifiés par un *Distinguished Name* unique ?
Q2	L'identifiant porté dans le certificat est-il construit à partir du nom du signataire ou d'un pseudonyme récupéré par l'autorité d'enregistrement ?
Q3	Lorsqu'un pseudonyme est utilisé, est-il identifié comme tel ?

Utilisation de noms explicites

Q4	Les procédures concernant le caractère explicite des noms sont-elles appliquées par le prestataire des services de confiance ?

Unicité des noms

Q5	Les procédures relatives aux règles d'unicité du nommage garantissent-elles l'unicité d'un même nom au sein d'un même domaine ?
Q6	L'unicité du *Distinguished Name* porté dans le certificat d'un signataire est-il assuré dans le domaine de sécurité tout au long du cycle de vie des autorités de certifications mises en œuvre par le prestataire des services de confiance ?
Q7	Les procédures permettant de s'assurer qu'un DN contenu dans un certificat ne peut être attribué à un autre signataire, durant le cycle de vie d'une autorité de certification, sont-elles formalisées, documentées et mises à jour ?

Validation initiale de l'identité

Méthode pour prouver la possession de la clé privée

Q8	Les méthodes permettant de garantir que le signataire possède la clé privée correspondante à la clé publique contenue dans le certificat sont-elles formalisées, documentées et à jour ?
Q9	La procédure permettant au prestataire de services de confiance de s'assurer que les signataires qui génèrent eux-mêmes leurs paires de clés utilisent un dispositif sécurisé de création de signature électronique est-elle formalisée, documentée et mise à jour ?

Q10	Au cas où la paire de clés du signataire est générée par le prestataire de services de confiance en dehors du dispositif sécurisé de création de signature (appartenant au signataire), le module cryptographique utilisé par le prestataire est-il conforme à la procédure faisant l'objet de la question précédente ?

Validation de l'identité de l'autorité

Q11	Les procédures administratives pour l'authentification d'un organisme sont-elles formalisées, documentées et à jour ?
Q12	Les procédures de contrôle du mandataire et de contrôle de l'authentification sont-elles formalisées, documentées, mises à jour et appliquées ?
Q13	Au cas où un système d'information est utilisé comme support à l'authentification d'un organisme, la procédure définit-elle un niveau de garantie équivalent à une authentification par contact direct ?
Q14	Au cas où le demandeur est une personne physique ayant une relation définie avec une personne morale identifiée dans le cadre des attributs des certificats, l'autorité d'enregistrement vérifie-t-elle les éléments suivants : • Nom complet du demandeur • Date et lieu de naissance du demandeur • Raison sociale et statut juridique de la personne morale correspondante • Numéro d'identification de la personne morale correspondante • Document officiel définissant le lien entre la personne physique et la personne morale
Q15	Le demandeur donne-t-il une adresse physique permettant de le contacter d'une manière vérifiable ?

Validation de l'identité du demandeur ou du mandataire

Q16	Les procédures administratives de validation de l'identité du demandeur ou du mandataire et les modes de transfert de cette information sont-ils formalisés, documentés et à jour ?
Q17	Au cas où un système d'information est utilisé comme support à l'authentification d'un organisme, la procédure définit-elle un niveau de garantie équivalent à une authentification par contact direct ?
Q18	La procédure de contrôle de l'identité du signataire, lorsque celui-ci est le demandeur existe-t-elle et est-elle documentée ?

Q19	La procédure de contrôle de l'identité du signataire, lorsque celui-ci n'est pas le demandeur existe-t-elle et est-elle documentée ?
Q20	La procédure d'authentification d'individus opérée par l'autorité d'enregistrement fait-elle appel aux informations suivantes : • Nom du demandeur • Date de naissance du demandeur • Numéro d'identification nationale du demandeur
Q21	La procédure permettant d'identifier un mandataire et de vérifier ses pouvoirs existe-t-elle et est-elle documentée et à jour ?

Identification et validation d'une demande de renouvellement d'une bi-clé

Certificat en fin de validité

Q22	La procédure de demande de régénération de certificat en fin de validité est-elle formalisée, documentée et à jour ?
Q23	La procédure d'authentification du signataire en cas de régénération du certificat en cas d'expiration est-elle formalisée, documentée et mise à jour ?
Q24	La procédure d'authentification du signataire en cas de demande de régénération signée par sa clé privée arrivant en fin de validité est-elle formalisée, documentée et mise à jour ?
Q25	Les procédures mentionnées dans cette sous-section permettent-elles de garantir les engagements relatifs aux mesures conservatoires et le niveau de sécurité requis ?

Certificat révoqué

Q26	La procédure de demande de régénération de certificat après révocation est-elle formalisée, documentée et à jour ?
Q27	Les moyens mis en place permettant la régénération des clés après révocation sont-ils adaptés et suffisants ?
Q28	L'autorité d'enregistrement vérifie-t-elle que l'identité et les attributs du signataire à inclure dans le nouveau certificat sont toujours valides ?
Q29	L'autorité de certification vérifie-t-elle que la sécurité cryptographique est toujours acceptable dans le cadre de la politique de certification pour toute la période de validité du certificat ?

Q30	L'autorité de certification vérifie-t-elle qu'il n'existe aucune indication suggérant que la clé privée du signataire a été compromise ?

Identification et validation d'une demande de révocation

Q31	Les procédures d'authentification d'une demande de révocation sont-elles formalisées, documentées et à jour ?
Q32	Les procédures d'authentification d'une demande de révocation imposent-elles une restriction de l'authentification du demandeur aux cas suivants : • signature de la demande par l'utilisation de la clé privée du demandeur • présence physique du demandeur auprès de l'autorité d'enregistrement • utilisation de la même procédure que lors d'un premier enregistrement auprès du prestataire de services de confiance
Q33	Les procédures d'authentification d'une demande de révocation sont-elles appliquées d'une manière effective et systématique ?

STE-3-2 : Critères techniques

Standards et mesures de sécurité pour les modules cryptographiques

Q34	Conformité à la norme ETSI EN 319401: General Policy Requirements for Trust Service Providers
Q35	Conformité à la norme ETSI EN 319 403: Norme européenne "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers"
Q36	Conformité à la norme ETSI EN 319411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
Q37	Conformité à la norme ETSI EN 319411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
Q38	Conformité à la norme ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
Q39	Conformité à la norme ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
Q40	Conformité à la norme ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
Q41	Conformité à la norme ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
Q42	Conformité à la norme ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
Q43	Conformité à la norme IETF RFC 3647 —(Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framwork) à laquelle doit se conformer le prestataire tout en se basant sur la « politique de certification de référence » « PC-type »
Q44	Infrastructures à clés publiques telles que précisées dans la recommandation UIT-T X.509 (Technologies de l'information - Interconnexion des systèmes ouverts - L'annuaire : cadre général des certificats de clé publique et d'attribut)

Q45	Le format d'un certificat électronique est celui de la norme ISO/IEC 9594-8 ou recommandation UIT-TX.509 v3
Q46	Algorithmes à clés publiques tels que décrits dans le standard IEEE. P1363 — Standard Spécifications For Public Key Cryptography, pour un système appartenant aux trois (03) familles d'algorithmes de cryptographie asymétrique : a. Logarithme discret : Diffie-Hellman, Menezez-QuVanstone (MQV), DSA avec SHA-1 ou version évoluée, Nyberg-Rueppel ; b. Factorisation des grands entiers : RSA tel que décrit dans ANSI X9.31, RSA Encryption, Rabin-Williams c. Courbes elliptiques : ECDSA (Elliptic-Curve DSA)
Q47	Conformité aux standards pour la cryptographie à clé publique : RSA PKCS (Public Key Cryptography Standard) : ✧ PKCS#1 RSA Cryptography Standard (1024, 2048 bit) ; ✧ PKCS#3 DI ffie-Hellman Key Agreement Standard ; ✧ PKCS#5 Password Based Cryptography Standard ; ✧ PKCS#6 Extended-Certificate Syntax Standard ; ✧ PKCS#7 Cryptographic Message Syntax Standard ; — PKCS#8 Private Key Information Syntax Standard ; ✧ PKCS#9 Selected Attribute Types ; ✧ PKCS#10 Certification Request Syntax Standard ; ✧ PKCS#11 Cryptographic Token Interface Standard ; ✧ PKCS#12 Personal Information Exchange Syntax Standard ; ✧ PKCS#13 Elliptic Curve Cryptography Standard ; ✧ PKCS#15 Cryptographic Token Information Format Standard.
Q48	Conformité aux recommandations FIPS (Federal Information Processing Standard): ✧ FIPS 180-3, Secure Hash Standard ; ✧ FIPS 186-3, Digital Signature Standard ; ✧ FIPS 140-2, Security Requirements for Cryptographic Modules (niveau 3) pour la sauvegarde de la clé privée du prestataire ; ✧ FIPS 198-1, the Keyed-Hash Message Authentication Code (H MAC) ; ✧ FIPS 197, Advanced Encryption Standard.
Q49	Standards pour la fourniture de service d'horodatage :

	a. La fourniture de services d'horodatage doit être conforme à la référence I ETF RFC 3161 : Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). b. ETSI – EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps.
Q50	Les modules cryptographiques utilisés par le prestataire ont-ils fait l'objet d'une analyse de leurs mécanismes cryptographiques lors de l'évaluation en vue de leur certification ?

Contrôle de la clé privée par plusieurs personnes

Q51	Les procédures de gestion et de contrôle des clés font-elle appel à au moins deux (02) personnes habilitées ?
Q52	Les procédures de gestion et de contrôle des clés font-elle appel, pour les fonctions à caractère fortement sensible, à des mécanismes à seuil (*k* parmi *n* avec *n*>2) ?
Q53	Les noms des personnes portant des parts de secret dans l'entreprise sont-ils clairement indiqués dans un procès-verbal ? Les parts sont-elles partagées dans le respect de la cohérence avec les profils de ces personnes ?
Q54	Les procès-verbaux relatifs aux opérations de gestion et de contrôle des clés montrent-ils que les points mentionnés dans les trois (03) questions précédentes sont respectés ?

Séquestre de la clé privée

Q55	Le séquestre des clés des signataires et des entités du domaine de confiance couvert par le prestataire de services de confiance est-il impossible d'une manière vérifiable ?

Copie de secours de la clé privée du prestataire de confiance

Q56	Les conditions de conservation des clés privées sont-elles documentées avec le niveau de précision requis ?
Q57	Quel est le niveau de sécurité (en termes d'intégrité et de confidentialité) du dispositif qui conserve les copies de secours des clés privées ?
Q58	Ce niveau de sécurité est-il égal ou supérieur à celui des clés privées en cours d'utilisation ?

Q59	Quand un certificat du prestataire n'est plus valide (révocation ou expiration), la clé privée correspondante est-elle détruite ou conservée de manière qui rend impossible toute remise en usage ?
Q60	Au cas où le prestataire de services de confiance utilise un module cryptographique pour y enregistrer des copies de ses clés, est-il conforme aux dispositions de la sous-section *Niveau d'évaluation sécurité du module cryptographique* du présent document ?

Archivage des clés privées

Q61	Le procédé d'archivage des clés privées rend-il impossible tout usage de ces clés (à l'exception des procédés d'investigation) ?
Q62	Quel est le niveau de sécurité (en termes d'intégrité et de confidentialité) du dispositif qui conserve les copies d'archive des clés privées ?
Q63	Ce niveau de sécurité est-il égal ou supérieur à celui des clés privées en cours d'utilisation ?
Q64	Au cas où le prestataire de services de confiance utilise un module cryptographique pour y enregistrer des copies de ses clés, existe-t-il un contrôle d'accès qui rend inaccessibles les clés en dehors de ce module ?

Transfert de la clé privée vers et depuis le module cryptographique

Q65	Le séquestre des clés des signataires et des entités du domaine de confiance couvert par le prestataire de services de confiance est-il impossible d'une manière vérifiable ?

Méthode d'activation de la clé privée

Q66	La procédure d'activation de la clé privée est-elle formalisée, documentée et à jour ?
Q67	Les rapports relatifs à l'activation de la clé privée montrent-ils que cette procédure est respectée ?
Q68	L'activation de la clé privée est-elle toujours réalisée par au moins deux (02) personnes ?

Méthode de désactivation de la clé privée

Q69	La procédure d'activation de la clé privée est-elle formalisée, documentée et à jour ?
Q70	Après sa désactivation, la clé privée est-elle conservée dans un lieu protégé ?
Q71	La désactivation de la clé privée est-elle faite automatiquement à la déconnexion de l'utilisateur ou après une période d'inactivité ?

Méthode de destruction des clés privées

Q72	La procédure de destruction des clés privées est-elle assortie d'un procès-verbal ?
Q73	La procédure de destruction prévoit-elle la destruction physique de la clé ainsi que de tous les supports physiques sur lesquels elle est enregistrée ?
Q74	Cette méthode rend-elle impossible toute utilisation des clés privées ayant fait l'objet de l'acte de destruction ?
Q75	Les personnes responsables de la procédure de destruction sont-ils identifiés d'une manière formalisée et documentée ?
Q76	Les procès-verbaux des actes de destruction des clés privées montrent-ils que la procédure est appliquée ?

Archivage des clés publiques

Q77	Les procédures de destruction des archives des clés publiques sont-elles conformes à leur niveau de sensibilité / classification ?
Q78	La durée de vie de conservation des clés publiques est-elle conforme à la réglementation Burkinabè ?

Génération et installation des données d'activation

Q79	La procédure de génération et d'installation des clés est-elle formalisée et documentée ?

Protection des données d'activation

Q80	Les moyens de protection définis pour les données d'activation permettent-ils de garantir un niveau de protection suffisant en confidentialité et en intégrité ?
Q81	La protection des données d'activation prend-elle effet de la génération de ces données jusqu'à leur distribution à l'utilisateur ?
Q82	L'utilisateur est-il informé des mesures à prendre pour protéger les données d'activation dont il dispose ?

STE-3-3 : Critères opérationnels

Exigences de sécurité technique spécifiques aux systèmes informatiques

Q83	Existe-t-il une procédure définissant les moyens de composition et de gestion des mots de passe ?
Q84	La procédure de mise à jour des logiciels de protection est-elle formalisée, documentée et à jour ?
Q85	La procédure de contrôle des postes de travail du prestataire des services de confiance est-elle formalisée, documentée et à jour ?
Q86	Les accès aux fonctions d'information et aux applications du système sont-ils effectivement restreints conformément à la politique de contrôle d'accès?
Q87	La journalisation des événements en fonction des rôles et des opérations est-elle mise en œuvre ?
Q88	La gestion des données d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlés par rôle et nom d'utilisateur) est-elle mise en œuvre ?
Q89	La gestion des comptes des utilisateurs est-elle mise en œuvre ?
Q90	L'authentification des utilisateurs des postes de travail est-elle mise en œuvre ?
Q91	La protection contre les virus informatiques et toutes formes de codes malveillants est-elle mise en œuvre ?
Q92	La protection des supports d'information contre les dommages, le vol et la compromission est-elle mise en œuvre ?
Q93	Le filtrage des entrées sorties réseau est-elle mis en œuvre ?
Q94	La mise en gestion des configurations du système est-elle mise en œuvre ?
Q95	La mise en œuvre des programmes utilitaires du système est-elle restreinte et strictement contrôlée ?
Q96	Les équipements de développement et de test sont-ils séparés des équipements de production ?
Q97	Les équipements identifiés comme sensibles, par les fonctions et les applications qu'ils mettent en œuvre, sont-ils isolés des autres postes de travail ?

Niveau d'évaluation sécurité des systèmes informatiques

Q98	Les systèmes informatiques utilisés dans le cadre des activités du prestataire des services de confiance ont-ils été mis en œuvre dans une optique de gestion des risques de sécurité ?
Q99	Des procédures d'installation des postes de travail prenant en compte les exigences de sécurité sont-elles formalisées, documentées et à jour ?
Q100	Des procédures d'utilisation des postes de travail prenant en compte les exigences de sécurité sont-elles formalisées, documentées et à jour ?

Mesures de sécurité des systèmes durant leur cycle de vie

Q101	Les moyens de protection des interconnexions vers les réseaux publics sont-ils conçus dans un souci de qualité, robustesse et fiabilité ?
Q102	Le prestataire protège-t-il ses systèmes informatiques et ses données contre les codes malveillants ?
Q103	Les données sensibles sont-elles protégées quand elles font l'objet d'un échange via des réseaux non sécurisés ?
Q104	Les procédures de gestion des incidents sont-elles formalisées, documentées et à jour ?
Q105	Les réseaux locaux du prestataire de services de confiance font-ils l'objet d'audit de sécurité d'une manière régulière ?
Q106	La montée en charge et le maintien des systèmes informatiques du prestataire des services de confiance font-ils l'objet d'un suivi ?

Mesures de sécurité liées au développement des systèmes

Q107	Une analyse des risques de sécurité est-elle conduite avant tout développement de systèmes informatiques ?
Q108	Le prestataire s'assure-t-il que chacune de ses entités satisfait aux exigences de sécurité de la norme ISO 15408 ou une norme équivalente ?
Q109	Les procédures prévoient-elles une réception technique à l'issue de tout développement ou toute évolution du système ?

Mesures liées à la gestion de la sécurité

Q110	Des procédures de contrôle portant sur les modifications (mise à jour, correction, patch,...) sont-elles formalisées, documentées et à jour ?
Q111	La sécurité du dispositif matériel est-elle protégée contre son altération par des tiers ou de toute autre manière lors de son transport ?
Q112	La sécurité du dispositif matériel est-elle protégée contre son altération par des tiers ou de toute autre manière lors de sa conservation ?
Q113	Les capacités de traitement et de stockage répondent-elles aux exigences de sécurité ?

STE-3-4 : Dispositions spécifiques relatives au format des certificats électroniques

Champ	Intitulé de l'exigence
Version	La valeur de ce champ doit être "2", indiquant qu'il s'agit d'un certificat version 3
Serial Number	Ce champ doit être généré de façon à ce qu'il soit unique pour chaque certificat
Signature	Doit être conforme aux règles et recommandations relatives aux dispositifs de signature du RGS-BF
Issuer	Doit être un Distinguished Name
Validity	Doit respecter les dispositions spécifiées dans RFC5280
Subject	Doit être un Distinguished Name
Subject Public Key Info	Doit être conforme aux dispositions spécifiées dans RFC3279 et aux règles et recommandations relatives du RGS-BF relatives aux algorithmes de cryptage et à la robustesse à la cryptanalyse
Unique Identifiers (issuer et subject)	Les PC Types du [RGS] imposant l'unicité des DN des champs Issuer et Subject au sein du domaine de l'AC, les champs Unique Identifiers ne doivent pas être utilisés.

STE-3-5 : Dispositions spécifiques relatives aux classes des certificats électroniques

Les classes de certificats reconnues dans le RGS-BF sont :

1. Classe 1 : la vérification du demandeur sur base de l'envoi d'une identité numérique.
2. Classe 2 : la vérification sur base d'une copie de la pièce d'identité du demandeur.
3. Classe 3 : la vérification sur base d'une présence physique du demandeur muni de l'original de sa pièce d'identité.

Le symbole + est ajouté à la classe si le certificat est soumis sur un support électronique sécurisé.

Le symbole EV est utilisé si le certificat comporte une preuve de l'identité légale du porteur de certificat.

Le terme "Wildcard" est ajouté à la classe d'un certificat d'authentification serveur si celui-ci porte sur plusieurs sous-domaines d'un domaine principal.

ANNEXE 7 HOM-1 : EXIGENCES RELATIVES A L'HOMOLOGATION DES SOLUTIONS DE SECURITE

HOM-1-1 : Démarche d'homologation

La démarche d'homologation consiste en cinq (05) étapes :

1. réception des dossiers d'homologation : consiste à traiter la demande d'homologation émanant d'une entité du périmètre du RGS-BF ;
2. définition de la cible d'homologation : un ensemble de fonctions devant être soumises à l'évaluation est identifié en fonction de la nature de la solution qui fait l'objet de l'homologation et du besoin exprimé dans la demande d'homologation ;
3. élaboration de la stratégie d'évaluation : les étapes dont consiste le processus d'évaluation de la solution sont identifiées à cette étape ;
4. mise en œuvre de l'évaluation : les tests faisant partie de la stratégie d'évaluation sont exécutés et documentés selon les dispositions prévues à cet effet ;
5. élaboration du rapport d'homologation : sur la base des résultats des tests d'évaluation, une décision est élaborée quant à l'attribution ou non du certificat d'homologation. Au cas où le certificat d'homologation est attribué, les risques résiduels liés à l'utilisation de la solution ayant fait l'objet de la démarche d'homologation doivent être clairement indiqués dans le rapport.

HOM-1-2 : Dispositions relatives aux niveaux d'homologation

Les tests prévus pour l'obtention d'un certificat d'homologation selon les niveaux définis par le RGS-BF sont définis selon la nomenclature des tests utilisée dans les Critères Communs (*Common Criteria*, CC) et les niveaux d'évaluation définis dans les niveaux d'évaluation de l'assurance (*Evaluation Assurance Levels*, EAL). L'équivalence entre les dispositions prévues dans le RGS-BF et les dispositions de ces deux (02) référentiels est donnée dans le tableau suivant.

Type d'homologation RGS-BF	Nomenclature CC	EAL		
		Niveau basique	Niveau moyen	Niveau robuste
Homologation relative à une spécification	ATE	1	3	4
	ALC	1	2	4
	AGD	1	3	4
Homologation relative à la robustesse des implantations cryptographiques	FCS	1	3	4
Homologation relative à la robustesse à une liste de vulnérabilités	AVA	1	2	3

ANNEXE 8 PRO-1 : EXIGENCES RELATIVES A LA PROTECTION PROACTIVE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

PRO-1-1 : Guide national d'utilisation des firewalls et politiques de filtrage associées

La politique de filtrage d'un firewall définit la manière dont il doit gérer le trafic réseau en se basant sur la politique de sécurité de l'entité bénéficiaire. Le filtrage peut être effectué sur la base des adresses IP, des plages d'adresses, des protocoles, des applications et du type du contenu.

1. Règles basées sur les adresses IP et les protocoles

La politique du firewall doit seulement autoriser les protocoles IP nécessaires au bon fonctionnement des services déployés par l'entité bénéficiaire. Les protocoles IP couramment utilisé sont ICMP, TCP, et UDP. Cependant, d'autres protocoles, tels que IPSec, peuvent être aussi gérés par le firewall si des services qui leurs correspondent sont déployés. En outre, ces protocoles doivent être autorisés seulement pour les hôtes qui en ont besoin.

a. Filtrage sur la base des adresses IP et autres champs de l'entête IP

La politique du firewall doit seulement autoriser les adresses IP sources et destinations nécessaires au bon fonctionnement des services déployés par l'entité bénéficiaire.
Les recommandations pour le filtrage basé sur les adresses IP sont listées ci-dessous :

- un trafic ayant une adresse IP source ou destination non valide doit être systématiquement bloqué ;
- un trafic entrant ayant une adresse source non valide doit être bloqué au périmètre du réseau ;
- un trafic sortant ayant une adresse destination non valide doit être bloqué au périmètre du réseau ;
- un trafic entrant ayant comme adresse destination privée doit être bloqué au périmètre du réseau ;
- un trafic sortant ayant une adresse source privée doit être bloqué au périmètre du réseau ;
- un trafic sortant ayant des adresses sources non valides doit être systématiquement bloqué ;
- un trafic entrant ayant l'adresse du firewall comme destination doit être bloqué . Des exceptions peuvent être envisagées si le firewall fournit des services de connexion directe pour le trafic entrant, tel que la connexion à un serveur d'authentification ou l'établissement d'un tunnel protégé ;
- un trafic contenant des informations de routage qui permettent aux systèmes de spécifier les routes que les paquets vont traverser de la source vers la destination doit être bloqué au périmètre du réseau ;

- un trafic provenant d'un domaine externe et dont les adresses destination sont des adresses de diffusion doit être bloqué au périmètre du réseau.

b. Filtrage sur la base du protocole IPv6

IPv6 est une version du protocole IP qui est de plus en plus déployée. Bien que le format et la taille de cette version diffèrent de ceux de la version IPv4, les règles de filtrage des firewalls doivent être appliquées au trafic IP au sens large sans en distinguer les versions.

Chaque entité bénéficiaire doit mettre en place un firewall capable de filtrer les trafics IPv4 (au sens des dispositions de la section précédente) et IPv6 (au sens des dispositions de la présente section) indépendamment du fait qu'elle déploie ou non des services utilisant IPv6.

Les firewalls opérant selon IPv6 doivent supporter les fonctionnalités suivantes :

- toute règle de filtrage basée sur des adresses IPv4 doit être possible à utiliser sur la base d'adresses IPv6 ;
- les interfaces d'administration doivent permettre aux administrateurs de cloner les règles IPv4 au contexte IPv6 ;
- le firewall doit être capable de filtrer le trafic ICMPv6 tel que spécifié dans la RFC 4890 "Recommendations for Filtering ICMPv6 Messages in Firewalls" ;
- le firewall doit être capable de bloquer les protocoles basés sur IPv6 tels que les protocoles de gestion des tunnels IPv6-à-IPv4 et IPv4-à-IPv6, Teredo, et "Intra-site Automatic Tunnel Addressing Protocol" (ISATAP). Des exceptions peuvent être prévues si ces protocoles sont nécessaires au bon fonctionnement des services déployés ;
- si la politique de l'entité bénéficiaire impose le blocage d'un trafic IPv6 entrant ou sortant, le firewall doit être capable d'appliquer le blocage selon les mêmes règles pour toutes les formes d'encapsulation d'un trafic IPv6 dans un trafic IPv4.

c. Filtrage sur la base des protocoles TCP et UDP

Tout trafic TCP ou UDP entrant doit faire l'objet de règles de blocage par défaut. Ainsi, seuls les trafics TCP et UDP autorisés à accéder aux domaines protégés seront explicitement configurés sur le firewall.

D'autre part, des règles de filtrage moins strictes doivent s'appliquer aux trafics TCP et UDP issus des domaines protégés de l'entité bénéficiaire puisque celle-ci autorise ses utilisateurs à accéder à une large variété d'applications déployées à l'extérieur du domaine en question ;

Le firewall doit permettre de signaler et de bloquer tout trafic TCP ou UDP destiné à un domaine protégé et qui ne respecte pas la syntaxe des entêtes de ces protocoles ou qui ne respecte pas les enchaînements d'échange de paquets spécifiées dans ces protocoles.

d. Filtrage sur la base du protocole ICMP

Souvent, des attaquants utilisent des commandes ICMP pour réaliser des attaques de reconnaissance ou pour détourner les flux d'un trafic réseau. Cependant, le protocole ICMP fournit un outil nécessaire pour les utilisateurs du réseau, notamment pour les fonctions liées aux tests et à la résolution des problèmes de connectivité.

Afin de contrecarrer les activités malveillantes basées sur l'exploitation du protocole ICMP, le firewall doit :

- bloquer tout trafic ICMP sortant ou entrant qui n'a pas été clairement autorisé par l'entité bénéficiaire, et ce au périmètre du réseau ;
- pour un trafic ICMP encapsulé dans le protocole IPv4, les messages ICMP de type 3 ne doivent pas être considérés dans les règles de filtrage (parce qu'ils sont nécessaires au diagnostic du réseau) ;
- pour un trafic ICMP encapsulé dans le protocole IPv4, un filtrage spécifique doit être élaboré en tenant compte du RFC 4890 "Recommendations for Filtering ICMPv6 Messages in Firewalls"
- la commande ping (echo request, ICMP code 8) doit être bloquée sur le trafic destiné aux domaines protégés puisqu'elle peut permettre aux attaquants de dresser la topologie du réseau interne de l'organisation.

e. Filtrage sur la base du protocole IPSec

La politique de sécurité doit indiquer si l'établissement des tunnels IPSec est autorisé (depuis ou vers les domaines protégés).

Au cas où le protocole IPsec est utilisé, les trafics ESP ou AH doivent être limités à un ensemble retreint d'adresses autorisées, et ce pour les trafics issus des domaines protégés ainsi que ceux qui leurs sont destinés.

2. Filtrage basé sur les protocoles de la couche application

Les firewalls applicatifs permettent de filtrer et de valider le trafic entrant avant qu'il ne puisse atteindre un serveur spécifique pour réduire le risque d'attaques exploitant les failles de la couche applicative, notamment celles conduisant à la saturation du serveur.

La décision de mettre en place ou non une politique de filtrage applicatif doit tenir compte des points :

- existence préalable d'un firewall supportant le filtrage à la couche application ;
- existence de menaces que les mécanismes de filtrage existants ne prennent pas en compte ;
- possibilité de mettre en œuvre les politiques de filtrage sur les serveurs dont elles font l'objet ;
- latence causée par la mise en œuvre d'un firewall applicatif ;
- facilité de mise à jour des règles de filtrage sur le firewall.

3. Filtrage basé sur l'identité de l'utilisateur

Les firewalls qui supportent les politiques de filtrages basées sur les identités des utilisateurs doivent être capables de journaliser les événements relatifs à ces politiques. En d'autres termes, une identité qui existera dans les fichiers journaux ne sera pas limitée à une adresse IP mais elle sera étendue à d'autres attributs.

Selon le niveau de protection requis, les mécanismes prévus dans les protocoles IPSec, SSL, TLS et NAC peuvent être utilisés.

4. Filtrage basé sur l'activité sur le réseau

Certaines organisations recommandent que les firewalls ferment les sessions de connexion établies par des utilisateurs au bout d'une période d'inactivité bien déterminée. Dans ce cas, la politique du firewall doit se baser sur le délai au bout duquel une connexion est considérée inactive.

Des politiques permettant d'appliquer un traitement spécifique (tel que le routage vers un segment spécifique) basé sur le débit peuvent aussi être mises en œuvre pour contrecarrer les attaques de saturation. Par exemple, un trafic ICMP dont le débit excède un seuil déterminé dans la politique du firewall peut être routé vers un segment spécifique pour être inspecté rigoureusement. Ces politiques assurent un bon compromis entre le niveau de protection qu'elles assurent et le niveau de résilience qu'elles garantissent.

5. Recommandations générales

Les recommandations générales sont les suivantes :

- la mise en place d'une politique de filtrage d'un firewall ne peut se faire qu'à l'issue de l'élaboration d'une analyse de risques ;

- l'usage des politiques de blocage par défaut est recommandé ;
- les politiques de filtrage doivent être basées, au moins, sur la syntaxe des protocoles qu'elles spécifient et des échanges des paquets correspondants ;
- un trafic portant des adresses IP non valides doit être systématiquement bloqué ;
- la gestion du trafic IPv6 doit être prise en considération systématiquement ;
- les applications autorisées à échanger du trafic doivent être identifiées pour que les règles correspondantes soient intégrées dans la politique du firewall.

L'entité bénéficiaire doit effectuer l'atténuation des menaces.

1.1. Recommandations relatives au logiciel antivirus

Les logiciels antivirus sont les solutions les plus déployées pour l'atténuation des menaces relatives à l'infection par des programmes malveillants. Une panoplie de marques de logiciels antivirus est disponible sur le marché et qui doivent intégrer les fonctionnalités suivantes sur l'ordinateur en question :

- effectuer un scan des éléments critiques tels que les fichiers de démarrage et les enregistrements d'amorcement ;
- effectuer l'examen en temps réel des actions ayant lieu sur l'ordinateur afin d'identifier les codes malveillants, ceci revient par exemple à vérifier les pièces jointes des emails échangés. D'une manière générale, le logiciel antivirus doit scanner tout fichier durant son téléchargement, ouverture et exécution afin de vérifier s'il est infecté par un virus ;
- inspecter toutes les actions relatives aux applications sujettes d'être un moyen d'infection par les programmes malveillants telles que les navigateurs, les clients de messageries et les logiciels de messagerie instantanée ;
- examiner les périphériques de stockages intégrés ou bien connecté à l'ordinateur en question pour identifier les éventuelles infections par les programmes malveillants. L'entité bénéficiaire peut imposer que tout périphérique de stockage amovible, tel que les clés USB, soit examiné par l'antivirus avant d'être utilisés sur les ordinateurs de son domaine ;
- identifier les différents types de programmes et codes malveillants ;
- désinfecter les fichiers atteints de programme malveillant par la suppression des sources d'infections ou bien par la mise en quarantaine des fichiers en question pour qu'ils soient examinés ultérieurement.

Afin de gérer les menaces liées à l'infection par les programmes malveillants, l'entité bénéficiaire doit considérer les recommandations détaillée ci-dessous.

1.1.1. Déployer un système antivirus (client et serveur)

- Un logiciel antivirus doit être installé sur tous les ordinateurs aussitôt que le système d'exploitation est installé ;
- une fois installé, le logiciel antivirus doit être mis à jour par les patchs disponibles, ce qui éliminera toute vulnérabilité présente dans le programme en soi ;
- par la suite, un scan complet doit être lancé pour analyser des potentielles infections sur la machine en question ;
- pour maintenir et renforcer l'efficacité du logiciel antivirus, sa base de signatures virales doit être périodiquement mise à jour par les signatures des récents programmes malveillants.

1.1.2. Mettre en œuvre un processus centralisé pour la gestion et le suivi du logiciel antivirus

Ce processus est à la charge d'un administrateur qui assure l'acquisition, la vérification, l'approbation et la distribution de signatures et mises à jour du logiciel antivirus au sein de l'entité bénéficiaire.

Les utilisateurs ne sont pas autorisés de désactiver ou de désinstaller le logiciel antivirus sur leurs machines.

L'administrateur du logiciel antivirus doit veiller à ce que toutes les machines de l'entité bénéficiaire déploient la dernière version de l'antivirus et qu'il soit configuré correctement.

1.1.3. Déployer plusieurs solutions antivirus sur les équipements critiques

Afin d'améliorer la prévention contre les programmes malveillants sur les machines critiques tels que les serveurs de messagerie, il est recommandé de leurs intégrer plus d'une solution antivirus.

Afin d'éviter le conflit que peut créer la coexistence de différentes solutions antivirus sur la même machine, il est recommandé de réserver chacune d'elles à un domaine séparé. Par exemple dans le cas d'un serveur messagerie, une solution sera réservée au serveur mail interne et une autre au serveur mail du périmètre.

1.2. Recommandations pour les mesures préventives basées sur les firewalls

Les mesures préventives basées sur les firewalls doivent être en conformité avec les dispositions de l'Annexe PRO-1-1.

1.3. Recommandations pour les mesures préventives basées sur le filtrage et l'inspection du contenu

Les entités bénéficiaires doivent déployer des techniques de filtrages et d'inspection du contenu afin d'atténuer les menaces relatives à la propagation de programmes malveillants par les emails.

Les entités bénéficiaires doivent déployer des techniques de filtrage des spam qui sont un moyen essentiel des attaques de fishing.

Les entités bénéficiaires doivent déployer des techniques de filtrage et d'inspection du contenu afin de réduire les menaces d'infection par les programmes malveillants qu'on trouve les sites web.

Les entités bénéficiaires doivent bloquer les fenêtres surgissantes sur les navigateurs.

Le filtrage des emails et du contenu web doit utiliser des mécanismes tels que les listes noires et les services de réputations afin de bloquer tout contenu provenant d'un domaine malveillant connu au préalable.

Les entités bénéficiaires ayant besoin d'un niveau élevé de sécurité ou qui sont installées dans des environnements à haut risque doivent utiliser des technologies de vérification de code sur les machines qu'elles détiennent.

1.4. Recommandations pour les architectures de défense

1.4.1. Protection du BIOS

La modification du BIOS par un logiciel malveillant est une attaque sophistiquée qui peut avoir comme cible l'entité bénéficiaire. Afin d'éviter ce type d'infection, il est recommandé de considérer le référentiel « NIST Special Publication 800-147 » qui fournit un guide de mise en œuvre de mécanismes de protection du BIOS.

1.4.2. Sandboxing (techniques d'isolation)

Le sandboxing est un modèle de sécurité qui permet d'exécuter un programme dans un environnement restreint afin de l'isoler des autres programmes et limiter les opérations qu'il peut effectuer sur la machine en question.

L'entité bénéficiaire est recommandée d'utiliser des sandbox pour prévenir les incidents relatifs aux infections par des programmes malveillants.

1.4.3. Ségrégation des navigateurs web

Etant donné que les sites web sont la source la plus probable d'infection par les programmes malveillants, il est recommandé que les utilisateurs de l'entité bénéficiaire utilisent deux (02) navigateurs web différents: le premier sera utilisé pour les applications relatives à l'exercice de l'entité en question et l'autre pour la navigation sur tout autre site web.

1.4.4. Virtualisation

L'entité bénéficiaire peut utiliser deux (02) systèmes d'exploitation : le premier sera consacré aux activités relatives à l'exercice de l'entité en question et l'autre pour toute autre activité. Pour le faire, elle aura besoin de mettre en œuvre des solutions de virtualisation.

ANNEXE 9 PRO-2 : EXIGENCES RELATIVES A LA PROTECTION REACTIVE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

PRO 2-1 : Règles et recommandations relatives à l'utilisation des Systèmes de Détection d'Intrusions

1. Introduction

Le présent document décrit les règles et recommandations à respecter par l'entité bénéficiaire lors du choix et de l'utilisation des systèmes de détection d'intrusions (IDSs).

2. Exigences générales

Avant de procéder à l'évaluation des IDSs, les entités bénéficiaires doivent définir les exigences à remplir par ces systèmes, qui varient selon l'entité et selon l'environnement opérationnel où va être déployé l'IDS.

2.1. Environnement réseau et système

Pour choisir un IDS compatible avec le système d'information et le réseau de l'entité bénéficiaire, les caractéristiques suivantes doivent être évaluées :

- ✧ Spécifications techniques du système d'information : architecture réseau et interconnexions aux réseaux externes, nombre de postes de travail et leur localisation, systèmes d'exploitation, services réseaux et applications pouvant nécessiter l'usage d'un IDS, autres systèmes non relatifs à la sécurité et auxquels l'IDS peut être intégré.
- ✧ Spécifications techniques des mesures existantes de sécurité : Implémentation existante d'IDSs, serveurs de journalisation et logiciels SIEM, logiciels antivirus et antispyware, logiciels antispam, pare-feux réseau, proxy et autres outils de filtrage de paquets, services de chiffrement, VPNs, SSL/TLS.

2.2. Objectifs

Après l'étude de l'existant, l'entité bénéficiaire doit formuler les buts et les objectifs attendus de l'usage de l'IDS. Les domaines suivants sont à considérer :

- ✧ Les types de menaces desquelles l'IDS va protéger l'entité bénéficiaire
- ✧ Les autres usages du système d'information ou du réseau à surveiller et qui ne sont pas considérés comme menaces de sécurité.

2.3. Politiques de sécurité et du système d'information

L'entité bénéficiaire doit réviser ses politiques des systèmes et de sécurité et reformuler leurs objectifs, les actions à prendre en cas de violation, pour décider de configurer l'IDS à les détecter ou non.

2.4. Exigences externes

L'entité bénéficiaire doit savoir si elle est sujette à des exigences supplémentaires imposées par une entité externe. Les exemples d'exigence incluent :

- ✧ Exigences de sécurité imposées par la loi.
- ✧ Exigences d'audit pour des pratiques de sécurité ou pour réaliser les vérifications nécessaires.
- ✧ Exigences d'accréditation.
- ✧ Exigences judiciaires pour des enquêtes sur des incidents de sécurité.

2.5. Contraintes de ressources

L'entité bénéficiaire doit évaluer ses ressources budgétaire et humaine. Des coûts relatifs au déploiement, à la configuration, à la formation du personnel, entre autres, sont à prévoir.

3. Exigences liées aux capacités de sécurité

L'évaluation des exigences de capacités permettent de choisir les produits IDS nécessaires et suffisants aux besoins de l'entité bénéficiaire.

3.1. Capacités de collecte d'informations

L'entité bénéficiaire doit identifier les capacités de collecte d'informations nécessaires à ses fonctionnalités de détection et d'analyse, et évaluer les produits IDS par rapport à ses besoins.

3.2. Capacités de journalisation

La qualité de journalisation affecte les résultats des analyses et l'exactitude des alertes. L'entité bénéficiaire doit s'assurer que les produits IDS :

- ✧ enregistrent au minimum les activités basiques tel que l'horodatage, le type d'évènement et son détecteur ;
- ✧ enregistrent des informations de support indiquant les détails de l'évènement ;
- ✧ permettent aux utilisateurs d'associer les entrées du journal avec les références externes correspondantes telles que les numéros Common vulnerabilities exposures (CVE).

3.3. Capacités de détection

L'entité bénéficiaire doit évaluer soigneusement les capacités de détection des produits IDS. L'évaluation inclut :

- ✧ Les types d'activités que les produits IDS analysent totalement et partiellement.

- ✧ Les types d'incidents que l'IDS peut identifier à savoir le déni de service, violation de politique, scan de ports, logiciels malveillants et l'utilisation non autorisée des protocoles ou applications.
- ✧ Son degré de détection pour les types d'incidents qu'il peut identifier.
- ✧ L'efficacité de sa configuration initiale.
- ✧ Son efficacité à détecter les évènement mal intentionnés connus, inconnus, et ceux cachés par des techniques d'évasion.
- ✧ Son aptitude à déterminer le succès ou l'échec d'une attaque.
- ✧ Les mécanismes de réponse qu'il offre.
- ✧ Les options de personnalisation disponible aux administrateurs.
- ✧ Son efficacité à utiliser des information d'autres IDSs et de corréler les évènements pour améliorer la mise en priorité des alertes.

4. Exigences de performance

Il existe toujours un compromis entre la détection et la performance. Les performances annoncées par les constructeurs se rapportent généralement au maximum de capacité et qui peut être dégradé après un changement de configuration. Ainsi, l'entité bénéficiaire doit bien connaitre les conditions de test ayant abouti aux critères de performance annoncés.

5. Exigences de gestion

5.1. Conception et mise en œuvre

L'entité bénéficiaire doit évaluer les aspects suivants :

- ✧ Fiabilité : présence de matériel et de logiciel de redondance, présence de plusieurs serveurs de gestion et capteurs de détection et fiabilité du processus de basculement entre eux.
- ✧ Interopérabilité : l'IDS doit interagir avec les sources de données, et les logiciels de gestion et d'analyse des journaux.
- ✧ Evolutivité : l'IDS doit supporter différents nombres de serveurs et de capteurs, différents niveaux d'activité , surveiller différents réseaux simultanément…
- ✧ Sécurité : s'assurer de la protection des données stockées, des communications entre les différents composants de l'IDS, de la sécurité des tâches d'authentification, de contrôle d'accès et d'audit réalisées lors de l'usage ou de l'administration de l'IDS, de la résistance de l'IDS aux attaques contre lui.

5.2. Opération et maintenance

- Usage quotidien : évaluer le fonctionnement au quotidien de l'IDS à savoir l'affichage des alertes, des évènements, des notifications et des rapports aux utilisateurs et aux administrateurs, l'utilisation des interfaces, le taux d'informations enregistrées facilitant les analyses,
- Maintenance : évaluer les mécanismes de maintenance disponibles (CLI, GUI, en local ou à distance), et les mesures de sécurité s'y afférant, évaluer les mécanismes de sauvegarde et de restauration des configurations, évaluer la robustesse de la gestion des outils de journalisation.
- Mises à jour : évaluer les mises à jour en terme de fréquence, d'authenticité, d'alignement avec les nouvelles menaces, de distribution et d'installation.

5.3. Formation, documentation et support technique

- Formation : évaluer les formations dispensées par les vendeurs (composants IDS, audience cible, outils d'apprentissage, formats, localisation).
- Documentation : évaluer la documentation disponible et ses formats (papier, électronique, à travers une console).
- Support technique : évaluer les contrats de support technique proposés par le vendeur en terme de coût et de portée.

PRO 2-2 : Règles et recommandations relatives à l'utilisation des systèmes de réaction aux codes malveillants

L'entité bénéficiaire doit mettre en œuvre les mécanismes appropriés pour la réaction aux incidents relatifs à l'infection par des logiciels malveillants. La réaction à ces incidents doit prendre en considération la sévérité de l'infection et doit permettre de réduire son impact, l'éradiquer, et assurer le rétablissement. Durant cette étape, il est parfois nécessaire de revenir à la phase d'analyse afin de vérifier si d'autres infections ont eu lieu.

Une fois l'incident maitrisé, l'entité bénéficiaire doit générer un rapport qui fournit les détails de l'incident à savoir sa cause, son impact ainsi que les mesures et les procédures à mettre en place afin d'éviter sa reproduction.

2. Préparation aux incidents relatifs

L'entité bénéficiaire doit renforcer et maintenir les capacités en matière de lutte contre les programmes malveillants et ceci consiste à maitriser les types de ces programmes, leurs méthodes de propagation et la nature de l'infection qu'ils peuvent causer.

L'entité bénéficiaire doit désigner une équipe de travail qui soit responsable de la coordination de la réponse aux incidents relatifs à l'infection par des programmes malveillants.

L'entité bénéficiaire doit acquérir les outils nécessaires (logiciel et matériel) qui lui permettront de maitriser les incidents relatifs à l'infection par des programmes malveillants.

3. Détection et analyse

3.1. Identifier les caractéristiques des logiciels malveillants

L'entité bénéficiaire doit mettre en place les ressources nécessaires qui assurent la détection rapide des incidents afin de minimiser leurs étendues et leurs dégâts.

L'équipe de travail doit analyser tout incident suspect afin d'affirmer s'il est causé par un logiciel malveillant.

3.2. Identification des cibles infectées

L'entité bénéficiaire doit identifier toutes les machines infectées afin qu'elles soient traitées. Etant donné le nombre énorme de menaces relatives aux programmes malveillants, l'identification des machines infectées doit être conduite par un moyen automatisé. L'entité bénéficiaire doit identifier les cibles infectées et prévoir plusieurs stratégies et outils de mise en œuvre de la réponse.

L'entité bénéficiaire doit indiquer les informations qui serviront à l'identification des machines infectées et où peuvent-elles être enregistrées.

Les techniques d'identification des machines infectées que l'entité bénéficiaire peut déployer se répartissent selon les catégories détaillées dans ce qui suit.

3.2.1. Identification par investigation digitale

Des enregistrements sur les activités suspectes effectuées par les logiciels malveillants peuvent être extraits à partir des fichiers journaux des applications de sécurité déployées dans l'entité bénéficiaire. Les fichiers journaux indiquent aussi si la sécurité a été compromise.

Dans le cas où ces preuves sont introuvables, l'entité bénéficiaire doit investiguer les sources suivantes :

- les fichiers journaux du serveur DNS ;
- les fichiers journaux des serveurs applicatifs tels que les serveurs web et email ;
- les outils d'investigation du réseau tels que les outils de capture des paquets ;
- les fichiers journaux des équipements réseaux tels que les firewalls et les routeurs.

3.2.2. Identification active

L'identification active des machines infectées peut être mise en œuvre par les méthodes suivantes :

- Automatisation de la sécurité : il s'agit d'utiliser les technologies de suivi continu telles que le control d'accès pour chercher dans les caractéristiques de la machine des signes d'infection.
- Définition des signatures appropriées pour des systèmes IDS ou IPS installés sur le réseau : généralement cette technique offre un moyen efficace d'identification des machines infectées.

- Mise en œuvre des outils de capture des paquets et des analyseurs de protocoles : il s'agit de configurer ces outils pour leurs permettre d'analyser seulement le trafic réseau présentant des anomalies probables d'être causées par l'activité d'un logiciel malveillant.

3.2.3. Identification manuelle

L'approche manuelle ne doit être considérée que si les deux (02) approches susmentionnées ne peuvent pas être mises en œuvre. Cette technique consiste à fournir aux utilisateurs des informations concernant le comportement du programme malveillant et de leurs demander de vérifier si leurs machines présentent des signes qui correspondent à cette infection.

3.3. Priorité de réponse aux incidents

L'entité bénéficiaire doit attribuer aux logiciels malveillants qui peuvent se propager rapidement tels que les vers et causer un dégât démesuré en un peu de temps une haute priorité de réponse.

D'autres infections qui atteignent des machines isolées doivent avoir une priorité réduite.

3.4. Analyses des programmes malveillants

L'équipe de travail sur les incidents relatifs à l'infection par des logiciels malveillants doit effectuer une analyse profonde du logiciel malveillant détecté. Pour ceci, l'équipe doit acquérir une copie du programme, l'installer sur une machine isolée, et le soumettre à des tests de simulation.

4. Confinement

4.1. Confinement par participation des utilisateurs

Dans le cas d'infection de large étendue, l'entité bénéficiaire doit fournir à ses utilisateurs les instructions à suivre pour identifier et communiquer une éventuelle infection et procéder à son éradication.

4.2. Confinement à travers la détection automatique

La majorité des incidents relatifs à l'infection par des logiciels malveillants sont automatiquement confinés en utilisant les solutions présentées dans l'Annexe PRO-1-2.

A part les logiciels antivirus, l'entité bénéficiaire peut déployer les solutions suivantes pour effectuer le confinement des infections :

- le filtrage de contenu ;
- les logiciels IPS ;
- les listes noires.

4.3. Confinement par la désactivation des services

L'entité bénéficiaire doit prévoir la désactivation des services que le programme malveillant exploite durant son activité.

4.4. Confinement par la désactivation de la connectivité

Afin de confiner l'incident détecté, il est parfois nécessaire de restreindre la connectivité réseau temporairement aux machines infectées.

5. Eradication

Durant la phase d'éradication, l'entité bénéficiaire doit s'assurer de la non reproduction de l'incident en question. Pour cela, elle doit suivre les recommandations suivantes :

- Si l'incident exploite des vulnérabilités de sécurité présentes sur les machines infectées alors le traitement de ces faiblesses fait partie de l'éradication.
- Combiner plusieurs solutions d'éradication quand ceci est nécessaire.
- Lors des incidents, renforcer les efforts d'éradications par des employés du département des technologies de l'information.
- Effectuer le formatage et la réinstallation de toutes les applications sur les machines qui ne peuvent pas être complètement désinfectées.

Les solutions de sécurité les plus répandues pour l'éradication sont :

- les logiciels antivirus ;
- les techniques de gestions des vulnérabilités ;
- les outils réseau de contrôle d'accès.

6. Rétablissement

Le rétablissement des incidents relatifs à l'infection par des logiciels malveillants repose sur les deux (02) aspects suivants :

1. arrêter les mesures de confinement ;
2. restaurer les services et les données sur les machines infectées.

7. Recommandations générales

L'entité bénéficiaire doit suivre les recommandations suivantes pour garantir sa résilience aux incidents relatifs à l'infection par des programmes malveillants :

- Modifier la politique de sécurité pour qu'elle prenne en considération ces incidents.
- Mettre à jour les systèmes d'exploitation et les applications afin qu'ils soient en conformité avec la politique de sécurité.
- Mettre en œuvre des programmes de sensibilisation destinés aux utilisateurs.
- Déployer des logiciels de détection des programmes malveillants.
- Reconfigurer les logiciels de détection des programmes malveillants quand ceci est nécessaire.

ANNEXE 10 PRO-3 : EXIGENCES RELATIVES A L'ACCREDITATION DES AUDITEURS DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

Accréditation des Auditeurs de Sécurité

1. Introduction

Le présent document liste les exigences nécessaires pour l'accréditation des auditeurs de systèmes d'information. Cette accréditation est effectuée par l'ANSSI. L'accréditation est valable pour trois (03) ans et concerne tous ou parties des types d'audit cités ci-après.

2. Classification des activités d'audits

- Audit de sécurité des systèmes d'information : il consiste à vérifier que les dispositifs matériels et logiciels de l'audité sont conformes aux exigences de sécurité dictées par l'état de l'art, aux normes en vigueur et les exigences internes de l'audité.
- Audit de code : il consiste à analyser une partie du code source et les outils de compilation pour découvrir des vulnérabilités pouvant avoir un impact sur la sécurité de la cible à auditer.
- Audit de vulnérabilités: il consiste mesurer le niveau de sécurité d'un système ou d'un périmètre défini, d'en déterminer précisément les failles de sécurité et de pouvoir ainsi définir le degré d'exposition aux risques et menaces externes afin de mettre en oeuvre un plan de remédiation avec des actions correctives.
- Test d'intrusion : il consiste à simuler le comportement réel d'une attaque pour identifier des vulnérabilités du système d'information. Cette activité doit être accompagnée par d'autres activités d'audit.
- Audit organisationnel : il consiste à vérifier que les procédures de sécurité définies par l'audité sont conformes à l'état de l'art et aux normes en vigueur.

3. Evaluation du prestataire d'audit

3.1. Exigences juridiques

- Le prestataire d'audit doit justifier d'un statut de personnalité morale pouvant être tenu juridiquement responsable de ses activités d'audit, et en particulier des dommages éventuels encourus.
- L'audit doit se faire dans le cadre d'une convention préalablement approuvé par l'audité. Ce dernier doit être informé de l'organisation de l'activité d'audit.
- Le prestataire d'audit doit respecter la législation en vigueur lors du traitement des informations sensibles (à caractères personnel, de propriété intellectuelle,…)
- Le recours par le prestataire d'audit à la sous-traitance doit être préalablement connu et accepté par l'audité et ce dans le cadre d'une convention documentée.

3.2. Exigences éthiques

Une charte d'éthique doit être tenue par le prestataire d'audit et signée par tous ses auditeurs, et stipulant que :

- ✧ L'activité d'audit doit être réalisée avec toute loyauté, impartialité et bonne foi en respectant le personnel et l'infrastructure de l'audité.
- ✧ Les auditeurs doivent communiquer tout contenu illicite découvert lors de l'audit à l'audité, tout en s'empêchant de divulguer même aux autres auditeurs toute sorte d'information sans le consentement de l'audité.
- ✧ Le prestataire d'audit doit être en mesure de prouver que ses modalités de travail n'apportent aucune atteinte à son impartialité et ne provoquent aucun conflit d'intérêt à l'audité.
- ✧ Le prestataire d'audit doit s'empêcher de communiquer toute information concernant l'audit au public sans le consentement de l'audité.

3.3. Exigences techniques

Pour maintenir une équipe d'audit qualifiée permettant de mener à bien les conventions d'audit signées par le prestataire d'audit, ce dernier doit s'engager à :

- ✧ Recruter le nombre suffisant d'auditeurs qualifiés pour assurer les activités d'audit sujet de ses prestations.
- ✧ Assurer la bonne utilisation de ses outils par ses auditeurs et maintenir leur pertinence par des mises à jour continues.
- ✧ Maintenir à jour la compétence de ses auditeurs à travers des formations s'alignant avec la veille technologique, et ce à travers des formations continues, des séminaires, des abonnements à des revues spécialisées…

Les auditeurs évalués au titre de l'accréditation du prestataire d'audit doivent justifier de:

- ✧ Qualités personnelles : caractère adéquat, bonne communication orale, acuités pédagogiques, de synthèse et rédactionnelles, aptitude à évoluer et faire la veille sur ses compétences.
- ✧ Expérience professionnelle : formation impérative dans le domaine des systèmes d'information et de communications et de l'audit, avec préférablement un minimum de deux (02) années d'expérience dans les systèmes d'information et de communication, une année d'expérience dans la sécurité des systèmes d'information et une année d'expérience dans l'audit des systèmes d'information.

- ✧ Compétences techniques : couvrant les domaines de réseaux et protocoles, systèmes d'exploitation, couches applicatives, logiciels de sécurité, outils d'audit et de test d'intrusion, techniques d'ingénierie inverse.
- ✧ Compétences spécifiques à l'activité d'audit : maîtrise de la méthodologie d'audit décrite dans la norme ISO 19011, bonnes compétences dans au moins un types des activités d'audit (organisationnel, test d'intrusion, code, sécurité des systèmes d'information), aptitude à élaborer et adapter un rapport d'audit et des recommandations destinés à des audiences diverses (techniques, administratives,…)

4. Evaluation de l'activité d'audit

Le déroulement de l'activité d'audit doit se conformer dans ses grandes lignes aux directives de la norme ISO 19011.

4.1. Le contrat d'audit

Le contrat d'audit doit préciser les points suivant :

- ✧ Le périmètre : identifie le système audité, les livrables attendus en entrée et en sortie, les personnes impliquées par le prestataire d'audit et l'audité, les actions nécessitant une autorisation explicite ou la présence de l'audité.
- ✧ Etique de l'audit : inclut les termes de la charte d'éthique du prestataire d'audit, une clause de non divulgation d'informations sauf sous autorisation, sort des informations collectées à la fin de l'audit (modalités de restitution ou destruction…).
- ✧ Risques éventuels : pouvant résulter de l'activité d'audit et la présence ou non d'une assurance couvrant les dommages éventuels.
- ✧ Dispositions : les moyens mis à la dispositions de l'auditeur pour réaliser son activité et les outils utilisés par le prestataire d'audit (termes de titularisation ou propriété intellectuelle).
- ✧ Livrables et recommandations : contenu, forme, cible.

4.2. Préparation de l'audit

Cette phase précède le démarrage de l'activité d'audit et doit inclure un ensemble de préparatifs à assurer par la personne élue par le prestataire d'audit chef de l'équipe d'audit. Cette personne doit :

- ✧ Former une équipe d'audit qualifiée pour réaliser la prestation d'audit en question.
- ✧ Communiquer avec les personnes concernées chez l'audité pour préciser les modalités de l'audit.

- S'assurer de l'avertissement des entités concernées chez l'audité et de l'obtention de leurs accords.
- Elaborer un plan d'audit précisant : les objectifs, les critères, le périmètre technique et organisationnel, les dates, les lieux…
- Obtenir toute la documentation existante relative à la cible de l'audit.
- Réaliser une réunion formelle avec les responsables de l'audité pour confirmer les accords établis sur les modalités.
- Informer l'audité de l'intérêt des sauvegardes de données sur les machines à auditer.
- Obtenir une autorisation préalable dans le cas du test d'intrusion précisant les machines cibles, les noms de domaines, les adresses IP, les heures exclusives du test et la durée de l'autorisation.

4.3. Exécution de l'audit

Le déroulement de l'activité d'audit doit se conformer aux termes du contrat d'audit et des accords préétablis, à savoir le respect de la confidentialité des informations, du personnel et de l'infrastructure de l'audité, la déclaration immédiate à l'audité de la présence de vulnérabilités critiques, la restitution de l'état initial du système d'information à la fin de l'audit, la documentation de tous les constats et le traçage de toutes les actions, la présentation de preuves pour toutes les observations.

Les actions réalisées pendant l'audit varient selon le type d'audit à réaliser :

4.3.1. Audit de sécurité des systèmes d'information

L'auditeur doit vérifier :

- L'architecture et les interconnexions avec des réseaux externes.
- Les équipements réseaux et leurs configurations.
- Les équipements de sécurité et leur règles de filtrage ou de chiffrement.
- Les serveurs, les postes de travail, les équipements téléphoniques.
- Les systèmes d'exploitation, les systèmes de gestion des bases de données, les environnement de virtualisation.

4.3.2. Audit de code

L'auditeur doit disposer du code source aussi bien que de la configuration des compilateurs et de l'architecture du système d'information. Un entretien avec un développeur permettra de préciser le contexte de l'application et de cibler directement les parties critiques du code qui sont relatives aux fonctionnalités de sécurité à savoir : les mécanismes

d'authentification et de contrôle d'accès, les mécanismes de cryptographie, la gestion des utilisateurs, l'interaction avec les autres applications et avec le système de gestion de base de données. La recherche de vulnérabilités commence par celles les plus répandues dans les domaines de : injections SQL, débordement de tampon, inclusion de fichiers, cross-site scripting…

4.3.3. Audit de vulnérabilités

L'auditeur doit dérouler un processus au cours duquel les composants réseaux, les systèmes et les applications sont scannés dans le but d'identifier la présence de vulnérabilités connues sans pour autant les exploiter.

4.3.4. Test d'intrusion

Ce type d'audit demande la réalisation d'un test d'intrusion sur une cible en passant par une ou plus des étapes suivantes :

- Boite noire : l'auditeur dispose uniquement d'une adresse IP de la cible et de l'URL correspondant. L'auditeur doit réaliser une phase de reconnaissance en consultant les services DNS et en interrogeant les ports ouverts.
- Boite grise : l'auditeur dispose des privilèges d'un utilisateur standard.
- Boite blanche : l'auditeur dispose du maximum d'informations telles que l'architecture, le code, ...

L'auditeur doit prévenir l'audité avant l'exécution de toute action pouvant être nocive. Les vulnérabilités découvertes ne peuvent être exploitées que suite au consentement de l'audité. Les nouvelles vulnérabilités découvertes doivent être signalées à l'ANSSI.

1.1.1. Audit organisationnel

Il doit permettre de mesurer la conformité de la sécurité des systèmes d'information, évaluée à partir des référentiels, aux règlementations et législations en vigueur.

4.4. Fin de l'audit

Dans une réunion avec l'audité, l'auditeur l'informe des premiers constats et des vulnérabilités critiques nécessitant une intervention urgente, et ce sans attendre l'élaboration du rapport d'audit. Ce dernier est ensuite élaboré et contient : une synthèse des résultats, des vulnérabilités, du niveau global de sécurité, l'ensemble de

recommandations visant à résoudre les vulnérabilités identifiées. Une réunion de clôture permet de présenter le rapport d'audit et les recommandations.