Loi de Programmation Militaire 2014-2019

Première partie

TLS-SEC – 2020-2021

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

SOMMAIRE

Logistique	3
Introduction à la LPM	14
Mise en œuvre	29
Les règles	34
Piloter la gouvernance de la cybersécurité	37
Maîtriser les risques	41

AVERTISSEMENT

Le contenu et les opinions exprimés dans ce support et lors de cette présentation sont sous mon entière responsabilité et n'engage donc que moi. Même s'ils font beaucoup référence à mon employeur actuel, les retours sont basés sur toutes mes expériences.

Logistique du cours

- **Deux séances**
  - 07/12/2020 – 14h-15h45
  - 14/12/2020 – 14h-15h45
- **Support distribué a format électronique**
- **Evaluation**
  - QCM
- **Contact**
  - Julien.airaud@cnes.fr – 05 61 28 75 94

Attentes ?

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

Intervenant

Julien Airaud
Responsable du
programme Cybersécurité

@airaudj

julien.airaud@cnes.fr

ISO27001 Lead Implementer (by LSTI)
ISO27005 Risk Manager (by LSTI)
Membre de l'IAC et du CCSDS SEA-SEC Working Group
Animateur du COMET-CYB (https://www.comet-cnes.fr/cyb)

Parcours

Ingénieur SSI en cyber assurance

Architecte Réseaux Systèmes et Sécurité

Responsable des infrastructures EMEAR

Adjoint SSI au Directeur du Centres Spatial de Toulouse

Responsable du programme de Cybersécurité du CNES

Présentation du CNES

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

Agence de programmes et centre d'excellence technique

Créé en 1961, le CNES est un établissement public à caractère industriel et commercial

- Il propose au gouvernement la politique spatiale française et la met en œuvre au sein de l'Europe, dans un cadre international
- C'est un architecte système chargé d'innover et de concevoir les nouveaux systèmes spatiaux.

Le CNES a pour mission d'apporter une vision d'ensemble des solutions spatiales grâce à sa compétence système et à sa capacité d'innovation. Il est :

- à l'écoute des utilisateurs et de leurs besoins.
- au carrefour des laboratoires scientifiques/technologiques, des entreprises industrielles et de services.
- au service des besoins institutionnels et commerciaux en stimulant la recherche et l'innovation scientifique, technologique et industrielle et en soutenant la compétitivité des entreprises.

Le CNES développe de nombreuses coopérations le mettant au contact des meilleures compétences mondiales et contribuant à la politique étrangère de la France. Il participe ainsi à des projets d'envergure :

- dans le cadre de projets développés avec l'ESA et les pays européens : lanceurs, programmes Cosmic Vision et Earth Explorer de l'ESA, Copernicus de la Commission européenne …
- avec les acteurs majeurs du spatial : Etats-Unis, Inde, Russie, Japon, Chine…
- au travers de coopérations ciblées avec de nombreux partenaires : Israël, Mexique, Corée, Emirats arabes unis…

Au service de l'Europe pour :

- *Maîtriser l'espace de bout en bout*
- *Etre moteur dans la construction de l'Europe de l'Espace*

LE CNES

2,4 Mds € budget

2e budget mondial/hab

80% revient à l'industrie

PARIS (Les Halles) - 190 P

Siège du CNES

- Stratégie,
- Relations internationales,
- Administration

PARIS (Daumesnil) - 210 P

Lanceurs

- Etude, conception, développement des systèmes de lancement (Ariane, Soyouz, Vega,)

Préparation du futur

4 centres **2,400** salariés

TOULOUSE - 1720 P

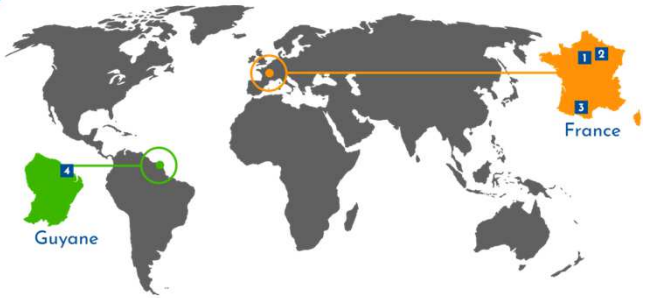
Centre Spatial de Toulouse

- Etude, conception, développement et contrôle des systèmes orbitaux
- Numérique et exploitation des données
- Préparation du futur
- Aire-sur-l'Adour : centre d'opération de ballons

GUYANE - 280 P

Centre Spatial Guyanais

- Ariane
- Soyouz
- Vega



LE CNES – SES MISSIONS

5 grands domaines d'intervention

ARIANE

Autonomie d'accès à l'espace est un enjeu de souveraineté garanti par la gamme des lanceurs européens.

SCIENCES

L'exploration et l'utilisation de l'espace s'appuient sur des développements technologiques d'envergure pour tenter de répondre aux questions fondamentales de l'humanité sur l'origine du système solaire, des galaxies et de la vie.

OBSERVATION

La planète Terre vit sous le regard constant des satellites qui l'observent, étudient ses caractéristiques physiques, son atmosphère, ses océans, ses terres émergées et fournissent des mesures indispensables pour la météorologie, l'océanographie, l'étude du changement climatique, l'aménagement du territoire.

TELECOMMUNICATIONS

Les satellites jouent un rôle irremplaçable pour les télécommunications à haut débit, la localisation, la collecte de données environnementales, la recherche et le sauvetage.

DEFENSE

L'observation à très haute résolution, l'écoute, les télécommunications hautement sécurisées, la surveillance de l'espace contribuent à la paix et à la sécurité des citoyens.

3 enjeux structurants

INNOVATION

Novateur et visionnaire de naissance, le CNES travaille à des projets spatiaux qui améliorent la vie des citoyens, répondant ainsi à des enjeux économiques et sociétaux.

© CNES/LE BRAS Gwenewan, 2018

CLIMAT

Si l'on veut comprendre, atténuer le changement climatique et s'y adapter, toutes les nations doivent se mobiliser ensemble et maintenant. 195 pays ont signé en décembre 2018 l'accord de Paris sur le climat dont le volet spatial a été impulsé par le CNES, car seuls les satellites peuvent nous permettre d'étudier le climat à l'échelle globale.

© CNES/PIRAUD Hervé, 2019

EXPLORATION

L'essor des applications spatiales et la diminution du coût des satellites et des lancements ouvrent de nouvelles possibilités à l'exploration spatiale. Les équipes du CNES s'investissent dans les missions les plus ambitieuses, de celles qui ne peuvent voir le jour qu'en coopération internationale.


© NASA/JPL Caltech, 2019

Stage !

Évolution du schéma directeur de cybersécurité

- Stage / 4-6 mois / TLS
- Recrutement.cnes.fr

Au sein de la Direction Centrale de la Sureté, la sous-direction Prescription COntrôle (DCS/PCO) est chargée de la définition des politiques de sureté (et de l'écriture des directives qui en découlent), de la spécification des mesures de protection à mettre en place par le CNES ainsi que du contrôle de leur mise en œuvre. La sous-direction, bi-localisé à Paris/Les Halles et à Toulouse, a de nombreuses interfaces au sein du CNES (experts sureté et autres structures du CNES) mais aussi à l'extérieur du CNES (autorité nationale, industriels du secteur).

Le Schéma Directeur de Sûreté du CNES a été consolidé en 2020 suite à la réorganisation des missions de sûreté du CNES. Il regroupe les aspects cybersécurité et sécurité / protection.

L'objectif du stage est :

- Dans un premier temps, de faire une cartographie et une revue du dispositif en place par rapport à la couverture de la menace et aux référentiels et bonnes pratiques du secteur.
- Cette revue permettra dans un second temps de proposer des pistes d'amélioration permettant la mise en place d'un système de management de la sécurité.

Le stage pourra débuter à partir du premier trimestre 2021.

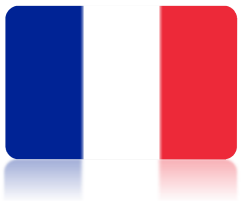
Introduction

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

Contexte

La dépendance de la société vis à vis des systèmes d'information est maintenant totale.

Face à l'augmentation en nombre et en complexité des attaques, les états et institutions réagissent pour se protéger, en conséquence, la réglementation s'étoffe:



- Dispositif de protection du potentiel scientifique et technique (PPST) du 2 novembre 2011
- Loi de Programmation Militaire (LPM) du 18 décembre 2013
- Instruction générale interministérielle 901 relative à la protection des systèmes d'information sensibles du 28 janvier 2015
- Directive européenne Network and Information Security (NIS) du 6 juillet 2016.

Organisation du dispositif

Premier ministre

Secrétariat général de la Défense et de la Sécurité nationale

Coordination interministérielle en matière de défense et de sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Autorité nationale en matière de sécurité et de défense des systèmes d'information

Un premier cadre de la LPM

SAIV

- Activités de production, distribution de biens ou de services **indispensables** à l'exercice de l'autorité de l'Etat, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la Nation, certaines activités sont considérées comme « d'importance vitale ».
- 12 secteurs définis par arrêté, chacun rattaché à un ministère coordinateur.

OIV

- Les opérateurs d'importance vitale sont désignés par le ministre coordonnateur du secteur qui les sélectionne parmi ceux qui exploitent ou utilisent des installations indispensables à la vie de la Nation. Les critères de choix et les objectifs de sécurité recherchés sont fixés par le ministère coordonnateur.

Les SAIV - Panorama

HUMAINE

Alimentation
Gestion de l'eau
Santé

REGALIENNE

Activités civiles de l'Etat
Activités judiciaires
Activités militaires
de l'Etat

ECONOMIQUE

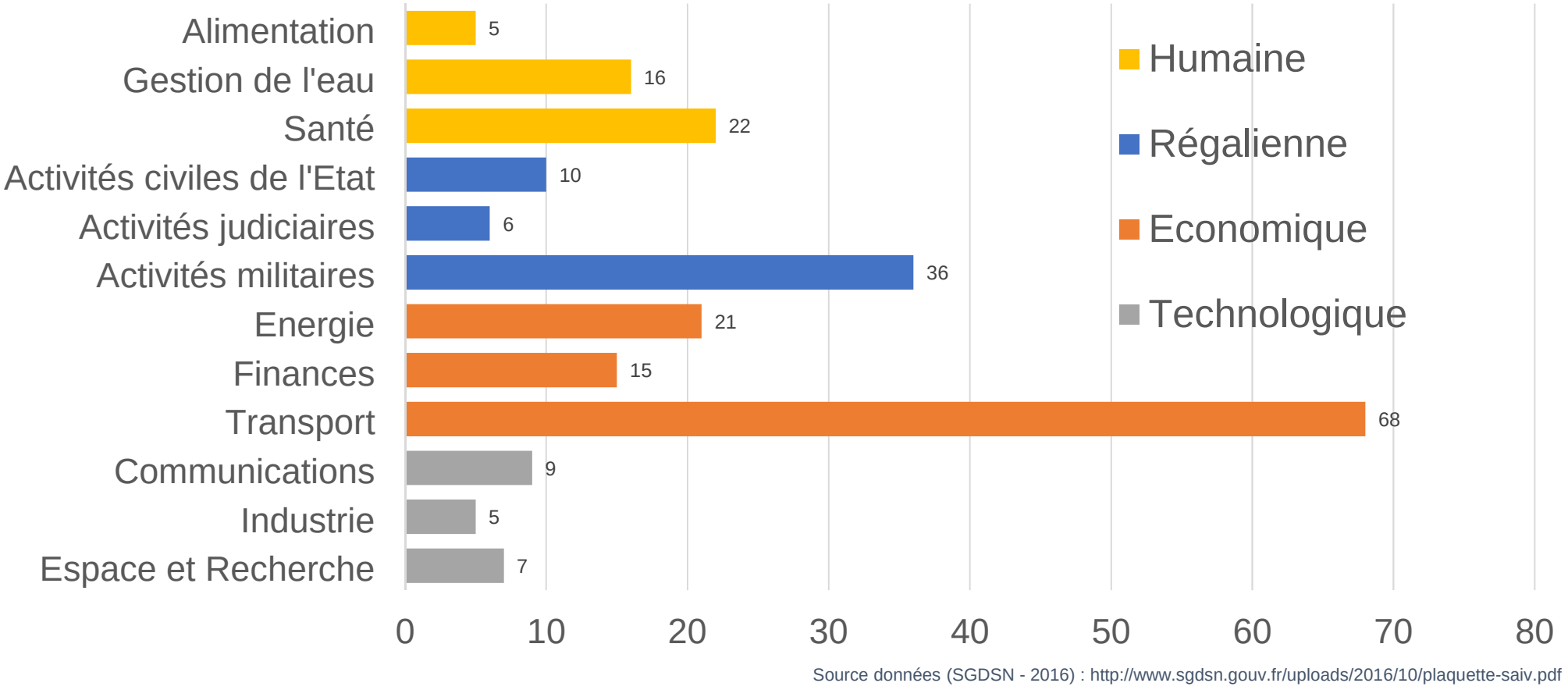
Energie
Finances
Transports

TECHNOLOGIQUE

Communications électroniques,
audiovisuel et information
Industrie
Espace et recherche

Source infographie (SGDSN - 2016) : http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf

Les SAIV – Volumes (2016)



Source données (SGDSN - 2016) : http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf

Calendrier

Juin 2006	Juin 2008	Juillet 2009	Avril 2013	Décembre 2013	Mars 2015	07/2016 →
Définition des SAIV	Livre Blanc Défense et Sécurité Nationale	Création de l'ANSSI	Livre Blanc Défense et Sécurité Nationale	Article 22 de la loi n°2013-1168 (codifié dans les articles L.1332-6-1 à L. 1332-6-6 du code de la défense)	Décret sur les prestataires de confiance	Publication des arrêtés sectoriels

Introduction à la Loi de Programmation Militaire

Utilisées depuis 1960, les LPM permettent de planifier les dépenses militaires sur plusieurs années dans un cadre budgétaire annualisé.

La loi n°2013-1168 du 18 décembre 2013 comporte deux séries de dispositions:

- **Programmatiques** pour les années 2014 à 2019.
- **Normatives** : elle prend diverses dispositions concernant la défense et la sécurité nationale, dont la cyberdéfense des OIV.
- Elle fait suite aux préconisation du livre blanc sur la défense et la sécurité nationale 2013
  - Commandé par le Président de la République en 2012, il fixe la stratégie française de défense et de sécurité nationale.

LIVRE BLANC
DÉFENSE ET SÉCURITÉ NATIONALE 2013

LPM - Chapitre IV (1/2)

Ce chapitre crée ou met à jour des articles du code de la défense.

Article 21 :

- Confère au Premier Ministre la définition de la politique et la coordination de l'action gouvernementale par sa disposition de l'Agence nationale de la sécurité des systèmes d'information.
- Il spécifie également une capacité de caractérisation des attaques et de neutralisation des effets par l'accès aux systèmes d'information à l'origine de ces attaques.

LPM - Chapitre IV (2/2)

Article 22 :

- Le PM définit les règles de sécurité nécessaires à la protection des systèmes d'information des Opérateurs d'Importance Vitale et des opérateurs qui participent à ces systèmes. Introduction des systèmes de détection qualifiés.
- Les OIV doivent informer sans délai le PM des incidents affectant leurs systèmes.
- Les OIV doivent se soumettre à des contrôles réalisés par l'ANSSI, des services de l'Etat ou par des prestataires qualifiés.
- En cas de crise, le PM peut décider de mesures à mettre en œuvre par les OIV
- Définit des sanctions pénales pour les dirigeants des opérateurs (150 000 €)comme les personnes morales responsables (750 000 €) en cas d'omission de protection ou de maintien de protection.

Un cadre de la LPM complété

SAIV

- Activités de production, distribution de biens ou de services **indispensables** à l'exercice de l'autorité de l'Etat, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la Nation, certaines activités sont considérées comme « d'importance vitale ».
- 12 secteurs définis par arrêté, chacun rattaché à un ministère coordinateur.

OIV

- Les opérateurs d'importance vitale sont désignés par le ministre coordonnateur du secteur qui les sélectionne parmi ceux qui exploitent ou utilisent des installations indispensables à la vie de la Nation. Les critères de choix et les objectifs de sécurité recherchés sont fixés par le ministère coordonnateur.

SIIV

- Systèmes pour l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population.
- Acteurs : OIV et Opérateurs publics ou privés qui participent à ces systèmes.

Les principes de la protection des SIIV

Focalisation sur les SIIV des OIV mais aussi sur l'écosystème (prestataires et produits qualifiés, sous-traitants).

Chaque SAIV fait l'objet d'un arrêté qui fixe pour le secteur:

- Les règles de sécurité (Annexe 1) et les délais de mise en œuvre (Annexe 2)
- Les modalités de déclaration des SIIV (Annexe 3)
- Les modalités de déclaration des incidents de sécurité (Annexe 4)

Quelques remarques sur la loi 2014-2019

La LPM a une approche à plusieurs facettes

- Initiative unique en Europe, le dispositif LPM a été élargi par la déclinaison nationale de la Directive NIS à partir de mai 2018.
- Approche de mise conformité dans laquelle l'importance de l'analyse de risques (au juste besoin) est toute relative (un livrable pour l'homologation).
- Protection axée sur la Disponibilité et l'Intégrité bien plus évident que pour la Confidentialité.

Impacts non négligeables pour les OIV

- Mise en conformité à leur frais,
- Nouvelle approche (conformité vs. gestion de risques) et en cumul avec d'autres réglementations,
- Pas de dérogation,
- Calendrier difficile à maîtriser jusqu'à l'homologation.

La Directive NIS

« La directive Network and Information System Security (NIS) poursuit un objectif majeur : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. Elle a été adoptée par les institutions européennes le 6 juillet 2016.Vote de l'Assemblée Nationale et application en France à partir de mai 2018. »

Source : site ANSSI

Les objectifs sont :

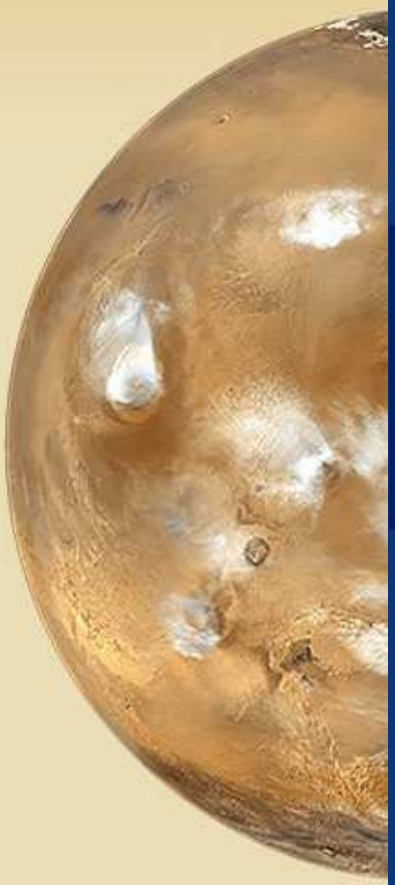
- Le renforcement des capacités nationales de cybersécurité (autorités nationales, Computer Security Incident Response Team - CSIRT - et stratégie nationale)
- Etablit un cadre de coopération volontaire entre Etats membres de l'UE.
- Renforcement de la cybersécurité des « Opérateurs de Service Essentiels » au fonctionnement de l'économie et de la société.
  - Cette notion étend la définition des OIV qui ne visait que le fonctionnement de la Nation.
- Instauration de règles européennes communes en matière de cybersécurité des prestataires de services numériques, notamment l'obligation de déclaration des incidents de sécurité.

LPM 2019 - 2025

Loi n°2018-607 Promulguée par P 13/07/2018

Objectifs de l'article 34:

- Renforcement des capacités de détection des attaques informatiques susceptibles d'affecter la sécurité des systèmes d'information de l'Etat, des autorités publiques et d'opérateurs publics et privés.
- Focalisation sur les Opérateurs de Communications Electroniques (OCE) et les hébergeurs.
  - Les OCE mettent en place des systèmes de détections
  - Lien direct entre ANSSI et OCE pour les attaques visant les OIV, les OSE ou les autorités publiques.
  - L'ANSSI peut déployer des dispositifs chez les OCE comme les hébergeurs.



La mise en œuvre

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

Processus

Identification et déclaration des SIIV

Réalisation des analyses d'impact des Systèmes d'Information (SI) de l'opérateur sur ses missions essentielles en cas de défaillance de sécurité (disponibilité intégrité et éventuellement confidentialité)

1. Il convient dans un premier temps de se référer à la Directive Nationale de Sécurité pour identifier les missions essentielles (ou vitales) à protéger.

- Attention à la divergence entre les intérêts de l'Etat et ceux de l'entreprise : il faut impliquer les métiers mais bien cadrer les discussions.
- Ces identifications permettent d'identifier une première liste de systèmes à partir de critères d'inclusion ou d'exclusion qu'il faut justifier.

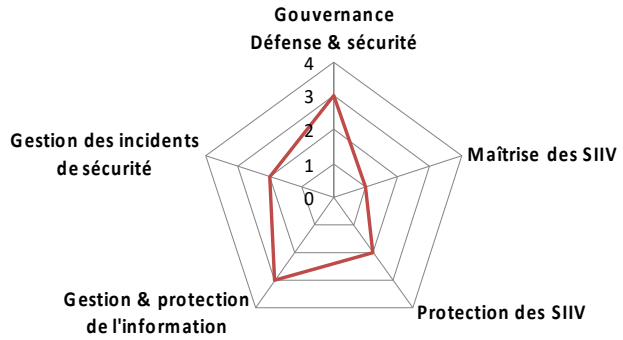
2. Chaque système est analysé individuellement

- Etude des impacts des atteintes en disponibilité et intégrité du SI isolé de son environnement. Contrairement à l'analyse de risques, la probabilité ne rentre pas en compte.
- Etude des redondances indépendantes ou mesures palliatives qui permettraient d'annuler ces impacts.
- Définir le système ou l'ensemble de sous-systèmes à déclarer et donc à mettre en conformité.

3. La pré-sélection des SI doit être confrontées et amendées à l'aide des types définis l'Annexe 3 de l'arrêté du SAIV de l'OIV (document Diffusion Restreinte).

- Exemple : centre de contrôles, réseau de communication, système de contrôle commande industriel (SCADA), systèmes classifiés, systèmes de contrôles d'accès physique.
- Si pour une catégorie, un OIV ne retient pas un système, il doit le justifier.

Analyse de la conformité du SIIV



Toujours avec les responsables du systèmes:

- Identifier les règles applicables au périmètre étudié :
  - Règles de niveau opérateur.
  - Règles de niveau système.
- Etudier le niveau de conformité ou de maturité par rapport aux référentiels constitués des règles de l'arrêté et de l'intégration des autres guides ou standards applicables.
- Identifier les priorités (Valeur/Effort)
- Etablir les mesures correctrices selon plusieurs axes
  - L'axe conformité → Un système ne peut être homologué que si toute les règles sont applicables.
  - L'axe temps → fonction des échéances applicables règle par règle.
- Etablir un plan de mise en conformité (transformation) par regroupement si possible.

Le plan ou projet de transformation

C’est un projet d’entreprise, pas uniquement du domaine de la SSI

- Le budget pluriannuel peut être conséquent, en investissement et en fonctionnement.
- Planning : Il est nécessaire de paralléliser les efforts, par règle, par système.
- De nombreux acteurs complémentaires sont impliqués
  - Dirigeants, Sûreté et Protection, RSSI, SSI, DSI, Métiers,etc.
- Il faut donc trouver des synergies entre les mesures de sécurité, regrouper les efforts entre SIIV (si possible).
- Etre concret le plus vite possible
  - Audit LPM
  - Utiliser un SSI pilote
  - Tester les solutions qualifiées le plus tôt possible.

Les règles

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

Organisation de l'Annexe 1

Etablies en concertation avec les OIV, les règles ont été publiées par les arrêtés sectoriels du 1/07/2016 au 1/10/2017 :

- Il existe très peu de variantes d'un secteur à l'autre.
- Les 20 règles rassemblent des bonnes pratiques en général, elles rendent cependant obligatoire les prestations ou produits qualifiés et font référence aux guides ANSSI (« bonnes pratiques »).
- Avec la publication des arrêtés démarrent les délais de mise en conformité
  - Application immédiate de l'obligation de déclaration
  - 3 mois pour déclarer les SIIV à l'ANSSI et déclarer un contact opérationnel à l'ANSSI
  - De 12 à 36 mois en fonction des règles et des secteurs

Les règles

5 thématiques:

- Piloter la gouvernance de la cybersécurité
- Maîtriser les risques
- Maîtriser ses systèmes d'information
- Gérer les incidents de cybersécurité
- Protéger les systèmes

20 Règles

+ Référentiels ANSSI :

- PASSI, PDIS, PRIS

+ Guides et méthodes ANSSI :

- Bonnes pratiques
- Méthode d'analyse de risques EBIOS

+ Instructions Interministérielles :

- II 901 sur la protection des SI sensibles
- IGI 1300 Protection du secret de la défense nationale

PILOTER LA GOUVERNANCE DE LA CYBERSÉCURITÉ

Piloter la gouvernance

PSSI (R1)

La PSSI doit intégrer les particularités liés aux OIV. Elle doit donc définir en plus:

- Les objectifs et orientations stratégiques en matière de SIIV,
- L'organisation de la gouvernance, rôles et responsabilités pour les SIIV,
- Le plan de sensibilisation de tous les salariés,
- Le plan de formation (des personnes à responsabilités particulières au sein des SIIV),
- Des procédures (…)

Elle doit être approuvée et faire l'objet d'un reporting annuel.

Au delà de la règle

Il est aussi nécessaire de revoir:

- Son référentiel SSI (directives et guides de sécurisation)
- Sa politique d'achat SSI
  - Intégration de prestations et produits qualifiés
  - Article 3-7 du code des Marchés Publics
  - Utilisation du guide de l'ANSSI
- Ses processus d'intégration de la SSI dans les projets
  - Pour établir et suivre les nouvelles règles et processus générés.

Indicateurs

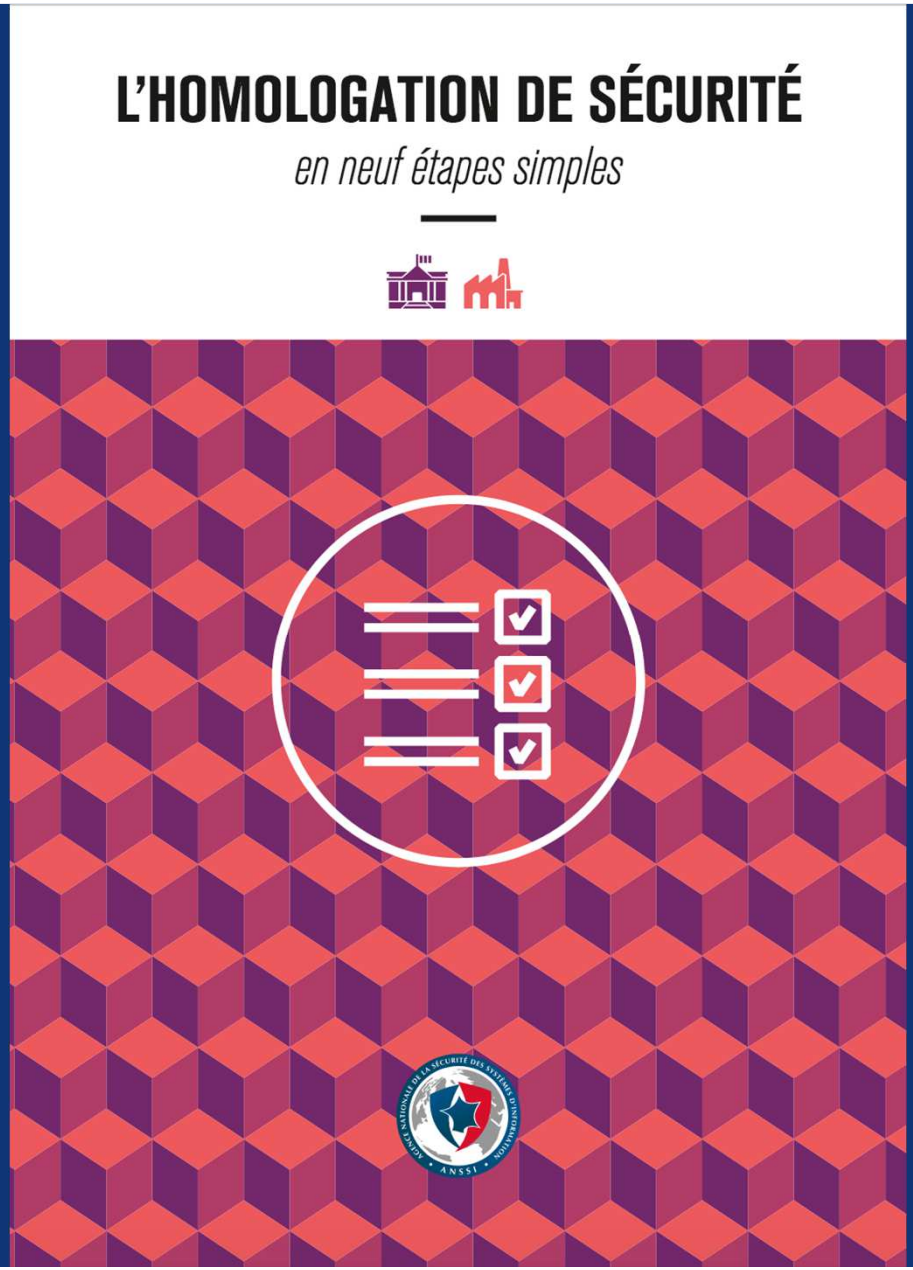
La règle n°20 définit des indicateurs à évaluer pour chaque SIIV et à communiquer à l'ANSSI une fois par an.

Indicateurs de MCS

- Suivi de systèmes en version non supportée ou non mis à jour ou corrigés depuis au moins 15 jours à compter de la disponibilité des patches

- Droits d'accès et authentification :
  - Usage des comptes partagés ou privilégiés
  - Pourcentage de compte sans possibilité de changement des secrets d'authentification
- Administration des ressources
  - Usage de comptes non dédiés à l'administration, de moyens ou flux non dédiés ou protégés pour l'administration

Conformément aux bonnes pratiques, les méthodes d'évaluation et les incertitudes doivent être précisées.



MAÎTRISER LES RISQUES

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

Introduction à l'homologation

L'homologation est une décision formelle prise par l'opérateur qui atteste que les risques liés à l'exploitation d'un SI sont acceptables. Ce processus vise à informer et responsabiliser dans le but d'une prise de décision.

Le processus d'homologation doit définir :

- Le référentiel réglementaire objet de cette homologation
- Le périmètre d'homologation (éléments fonctionnels, techniques, physiques
- Les acteurs, leurs responsabilités et l'organisation
- La liste détaillée des livrables (contenu, date de disponibilité, responsable)
- Le processus d'homologation (dépendances de produits ou prestations qualifiées, audit nécessaire)
- Le planning prévisionnel

Formes de l'homologation

En fonction des contraintes et de la sensibilité des systèmes, une homologation peut prendre plusieurs forme.

	Simplifiée	Intermédiaire	Complète
Exemple	Newsletter	Système de pointage	Système de lancement
Analyse de risque	Analyse Macro	Déroulé partiel de la méthode	Déroulé complet
Documents nécessaires	Déclaration de conformité	• Architecture • SecOps	Dossier complet (cf. planche suivante)
Evaluation du niveau de sécurité	Aucune	Automatisé complété des points d'attention	Audit complet
Maintien	Suivi automatique (scanner de vulnérabilités et de conformité), SOC standard	Simplifié + suivi manuel de certains points et quelques scénarios spécifiques en SOC Evaluation annuelle	Intermédiaire + nombreux scénarios spécifiques en SOC. Audits fréquents

L’homologation LPM

Elle a une durée de validité de 5 ans ou dépend de l’évolution du système.

L’homologation LPM requiert:

- Une analyse de risques et les objectifs de sécurité du SIIV
- Les mesures de sécurité appliquées
- Les rapports d’audit
  - L’objectif est de vérifier l’application et l’efficacité des des mesures de sécurité du SIIV et notamment les règles de l’arrêté applicable, évaluer le niveau de sécurité SIIV au regard des menaces et vulnérabilités connues.
  - Il comporte audit d’architecture, audit de configuration et audit organisationnel et physique et est réalisé selon les règles du référentiel PASSI (réalisé en interne ou par un prestataire qualifié).
- Les risques résiduels.