ROYAUME DU MAROC
ADMINISTRATION DE LA DÉFENSE NATIONALE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Guide d'homologation des systèmes d'information sensibles des infrastructures d'importance vitale

Informations

AVERTISSEMENT

Destiné à vous assister dans l'adoption d'une démarche cohérente et homogène pour la mise en conformité de la sécurité de vos systèmes d'information avec les règles de sécurité édictées par la loi 05.20 relative à la cybersécurité, ce guide élaboré par la DGSSI traite la démarche d'homologation des systèmes d'information sensibles des infrastructures d'importance. Il est destiné à évoluer avec les usages, mais aussi avec vos contributions et retours d'expérience. Les recommandations citées dans ce guide sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, la DGSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par la DGSSI doit être soumise, au préalable, à la validation du Responsable de la Sécurité des Systèmes d'Information (RSSI) et de l'administrateur du système concerné.

PERSONNES AYANT CONTRIBUÉ À LA RÉDACTION DE CE DOCUMENT :

Rédigé par	Version	Date
DGSSI	1.0	08/11/2021

ÉVOLUTION DU DOCUMENT :

Version	Date	Nature des modifications
1.0	08/11/2021	Version initiale

PUBLIC CONCERNÉ PAR CE DOCUMENT :

Responsable de l'infrastructure d'importance vitale
Responsable des systèmes d'information
Responsable de la sécurité des systèmes d'information

POUR TOUTE REMARQUE :

Contact	Email
DGSSI	contact@dgssi.gov.ma

Sommaire

I. Introduction et contexte 3
II. Acteurs de la démarche d'homologation 3
III. Périmètre de l'homologation 3
IV. Démarche d'homologation 4
1. Phase 1 : Planification de l'homologation 4
1.1. Planning 4
1.2. Document de planification de l'homologation 4
1.3. Dossier d'homologation 4
2. Phase 2 : Maîtrise des risques 5
2.1. Gestion des risques 5
2.2. Audit de la sécurité du système d'information sensible 6
2.3. Définition du répertoire des risques résiduels 6
3. Phase 3 : Décision d'homologation 6
3.1. Périmètre de l'homologation 7
3.2. Conditions accompagnant l'homologation 7
3.3. Durée de l'homologation 7
3.4. Conditions de suspension ou de retrait de l'homologation 7
4. Phase 4 : Suivi et maintien de l'homologation 7
4.1. Suivi de l'homologation 7
4.2. Maintien en conditions de sécurité 8
Annexe 1 : Description du système d'information sensible 9
Annexe 2 : Liste des documents pouvant être contenus dans le dossier d'homologation 10
Annexe 3 : Liste des menaces 12
Annexe 4 : Identification des actifs informationnels 14
Annexe 5 : Modèle de la décision d'homologation 16

I. Introduction et contexte

La loi n° 05-20 relative à la cybersécurité dispose dans son article 19 que tout système d'information sensible (SIS) d'une infrastructure d'importance vitale (IIV) doit faire l'objet de l'homologation de sa sécurité avant sa mise en exploitation.

Cette homologation est destinée à faire connaître aux responsables des IIV les risques liés à l'exploitation de leurs systèmes d'information sensibles.

Il s'agit d'une démarche qui aboutit à une décision, prise par le responsable de l'IIV. Cette décision constitue un acte formel par lequel il :

- atteste de sa connaissance du système d'information et des mesures de sécurité techniques, organisationnelles ou juridiques mises en œuvre ;
- accepte les risques qui demeurent, qu'on appelle risques résiduels.

Le présent guide détaille la démarche à suivre pour homologuer un système d'information sensible d'une infrastructure d'importance vitale et établi la forme et le contenu de la décision d'homologation.

II. Acteurs de la démarche d'homologation

L'homologation s'appuie sur plusieurs acteurs auxquels sont associés différents rôles et niveaux de responsabilité.

- **Responsable de l'infrastructure d'importance vitale**

Le responsable de l'IIV est la personne qui atteste de sa connaissance du SIS et des mesures de sécurité mises en œuvre, accepte les risques résiduels et signe la décision d'homologation.

- **Equipe de l'homologation**

Cette équipe peut regrouper des acteurs internes et externes à l'IIV. Elle est constituée notamment des personnes suivantes :

- Le responsable du système d'information ;
- Le responsable de la sécurité des systèmes d'information (RSSI) ;
- Le propriétaire du système d'information qui est responsable du développement, de l'intégration, de la modification et de la maintenance du système d'information ;
- Le responsable de l'exploitation du système d'information ;
- Les prestataires, en fonction de leur statut (interne ou externe), peuvent être intégrés à l'équipe de l'homologation, ou simplement consultés en cas de besoin. Ils remplissent un rôle d'assistance et peuvent produire des livrables qui seront versés au dossier d'homologation.

III. Périmètre de l'homologation

La délimitation du périmètre permet de déterminer et de caractériser précisément le SIS à homologuer. Ce périmètre comprend notamment :

- **La situation géographique et physique :**

Localisation géographique et caractéristiques des locaux.

- **Les 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 ;

- **Les 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.

Le périmètre peut évoluer au cours de la démarche d'homologation, mais il est recommandé d'aboutir rapidement à une délimitation stable de celui-ci.

En cas de systèmes interconnectés, il est recommandé d'appliquer une démarche d'homologation pour chaque système d'information sensible.

IV. Démarche d'homologation

La démarche d'homologation est le processus permettant de vérifier que la sécurité a été prise en compte avant la mise en service d'un système d'information sensible en appliquant les mesures de sécurité nécessaires et appropriées.

Elle permet de s'assurer que les risques pesant sur un système, dans le contexte de son utilisation, sont connus et maîtrisés de manière active, préventive et continue.

La démarche, de quatre phases, présentée dans ce guide, permet à l'équipe de l'homologation de préparer le dossier d'homologation et de le présenter au responsable de l'infrastructure d'importance vitale.

1. Phase 1 : Planification de l'homologation

1.1. Planning

L'homologation doit être prononcée préalablement à la mise en service opérationnelle du SIS. La démarche d'homologation doit donc être lancée en amont puis être intégrée à la phase d'étude, de conception ou d'acquisition.

Le planning doit contenir les échéances prévues pour les différentes phases de la démarche d'homologation, à savoir :

- La date de lancement de la démarche d'homologation ;
- La date de début et de fin de l'analyse des risques ;
- Les dates de remise des différents documents constituant le dossier d'homologation ;
- Les dates des réunions des différents acteurs de l'homologation ;
- Les dates des éventuels audits du système d'information ;
- La date prévisionnelle pour l'homologation du système d'information ;
- La date de mise en service du système.

1.2. Document de planification de l'homologation

Le document de planification de l'homologation représente la feuille de route sur laquelle s'appuie l'ensemble des acteurs de l'homologation pour mener à bien la démarche d'homologation. C'est un document qui, notamment :

- décrit le système d'information sensible en se référant l'annexe 1 ci-jointe ;
- désigne l'équipe de l'homologation ;
- délimite le périmètre de l'homologation ;
- fixe le planning de l'homologation ;
- fournit une estimation du coût de l'homologation.

1.3. Dossier d'homologation

Le dossier d'homologation, qui sera présenté au responsable de l'IIV, est constitué de l'ensemble des documents permettant à ce dernier de prendre la décision d'homologuer le système d'information. Il est alimenté pendant toutes les phases de l'homologation, essentiellement avec des pièces et justificatifs

nécessaires à la conception, à la réalisation, à la validation du projet ou à la maintenance du SIS après sa mise en service.

L'annexe 2 du présent guide présente la liste non exhaustive des documents pouvant être contenus dans le dossier d'homologation et en propose une description détaillée.

Il est à signaler que le contenu du dossier d'homologation, doit être marqué, protégé et conservé de manière appropriée.

2. Phase 2 : Maîtrise des risques

Le but de cette deuxième phase est d'identifier les risques pesant sur la sécurité du système d'information sensible visant à être homologué, de les hiérarchiser et de déterminer des objectifs qui permettront de diminuer certains d'entre eux et, à terme, de les amener à un niveau acceptable.

Cette phase consiste en :

1. La gestion des risques simplifié selon « le guide de gestion des risques de la sécurité des systèmes d'information » élaboré par la DGSSI ou détaillée selon une méthodologie reconnue (EBIOS, OCTAVE, MEHARI, etc.) ;
2. L'audit de la sécurité du système d'information sensible ;
3. La définition du répertoire des risques résiduels.

2.1. Gestion des risques

Le risque se présente comme étant la combinaison d'un événement redouté, susceptible d'avoir un impact négatif sur les missions d'une IIV, et d'un scénario de menaces. La gestion du risque est le processus permettant de déterminer les mesures de sécurité permettant de couvrir ces risques identifiés.

Le guide de gestion des risques précité détaille la méthodologie permettant d'effectuer le processus précité. Les étapes suivantes permettent de réaliser une analyse des risques d'une manière simplifiée :

1. Utiliser la liste des menaces courantes présentée à l'annexe 3 de ce guide. Ces menaces sont d'ordre accidentel, délibéré ou environnemental ;
2. Ecarter les menaces qui ne sont pas pertinentes dans le contexte du système d'information étudié ;
3. Déterminer les actifs informationnels primordiaux qui pourraient être affectés pour chaque menace conservée. L'annexe 4, ci-joint, présente les différents types d'actifs informationnels ;
4. Décrire l'impact négatif sur la disponibilité, l'intégrité et la confidentialité de cet actif et cela pour chaque lien identifié entre une menace et un actif informationnel. Il en découlera un scénario de risque.
5. Hiérarchiser les scénarios de risque obtenus, en identifiant les plus probables et ceux dont l'impact est le plus pénalisant.

A l'issue de ces 5 étapes, si un scénario aboutit à un impact très fort, il est recommandé d'envisager d'entreprendre une démarche d'analyse de risque plus approfondie (EBIOS, MEGHARI, OCTAVE, etc.).

Une fois l'analyse de risque achevée, il convient de définir, implémenter et contrôler les mesures de sécurité permettant de couvrir les risques identifiés.

L'équipe de l'homologation est appelée à se prononcer sur l'ensemble des risques afin de les amener à un niveau acceptable. Pour le traitement de ces risques, il convient de choisir parmi les options suivantes :

- Eviter le risque : en le contournant à travers des actions spécifiques (changer le contexte de telle sorte qu'on n'y soit plus exposé, supprimer l'activité l'amenant, etc.) ;
- Réduire le risque : en prenant des mesures de sécurité supplémentaire pour diminuer l'impact et/ou la vraisemblance ;
- Maintenir le risque : en supportant les conséquences éventuelles sans prendre de mesure de sécurité supplémentaire ;

- Transférer le risque : en le partageant avec un tiers (assureur, sous-traitant, etc.) capable de le gérer ou de l'assumer.

Il est à rappeler que plusieurs options peuvent être choisies pour chaque risque.

Suite à l'exécution de l'ensemble de ces étapes, il est impératif d'établir les documents ci-après, et de les joindre au dossier d'homologation :

- Le rapport d'analyse des risques et des objectifs de sécurité ;
- La liste des mesures de sécurité appliquées aux systèmes d'information sensible.

2.2. Audit de la sécurité du système d'information sensible

A ce stade, l'analyse des risques est effectuée, les objectifs de sécurités sont établis et les mesures de sécurité sont appliquées. Il est préconisé de mesurer l'écart entre les résultats de la gestion des risques et la réalité, en réalisant un audit de la sécurité du système d'information.

Selon les fonctions et les caractéristiques du système d'information, l'audit peut porter sur un ou plusieurs domaines d'audit, à savoir :

- Audit organisationnel et physique ;
- Audit de configuration ;
- Audit d'architecture ;
- Audit de code ;
- Tests d'intrusion ;
- Audit des systèmes industriels.

Cet audit peut intervenir à tout moment du cycle de vie du système : en amont, avant la mise en service voir au cours de la conception, mais également en aval, si le système est déjà opérationnel.

Les résultats de l'audit sont consignés dans un rapport dont les éléments à traiter sont énumérés au point 5 de l'annexe 2 de ce guide.

2.3. Définition du répertoire des risques résiduels

Les risques qui demeurent non couverts après la gestion des risques et l'application des recommandations issues du rapport d'audit, sont considérés comme des risques résiduels. Ils sont identifiés et inscrits dans un répertoire des risques résiduels qui précise les raisons justifiant leurs acceptations. Ce répertoire recense lesdits risques en indiquant leurs degrés de criticité, l'échéance pour l'atténuation de leurs impacts ainsi que les actions potentielles pouvant les corriger.

3. Phase 3 : Décision d'homologation

Durant la troisième phase, la décision d'homologation doit être concrétisée et signée par le responsable de l'IIV, et qui du point de vue de la sécurité :

- autorise formellement l'exploitation du système d'information, ou ;
- autorise provisoirement l'exploitation du système d'information sous réserve de respecter des conditions spécifiques (plan d'actions visant à maintenir et à améliorer le niveau de sécurité du système dans le temps), ou ;
- refuse l'attribution d'une autorisation d'exploiter le système d'information.

La décision d'homologation doit comprendre au minimum les éléments référencés ci-dessous :

1. Le périmètre de l'homologation ;
2. Les conditions accompagnant l'homologation ;
3. La durée de l'homologation ;
4. Le cas échéant, les conditions de suspension de l'homologation.

Le modèle de décision d'homologation est présenté en annexe 5, ci-jointe.

3.1. Périmètre de l'homologation

Il doit au moins tenir compte des éléments suivants :

- Périmètre géographique et physique (localisations géographiques, locaux, etc.) ;
- Périmètre fonctionnel et organisationnel (fonctionnalités, types d'informations traitées par le système et sensibilité, types d'utilisateurs, règles d'emploi, procédures, conditions d'emploi des produits de sécurité, etc.) ;
- Périmètre technique (cartographie, architecture détaillée du système, prestataires, etc.).

3.2. Conditions accompagnant l'homologation

Le responsable de l'IIV peut, en fonction des risques résiduels identifiés, assortir l'homologation de conditions d'exploitation ainsi que d'un plan d'actions visant à maintenir et à améliorer le niveau de sécurité du système d'information dans le temps.

3.3. Durée de l'homologation

L'homologation doit être décidée pour une durée maximale de trois (03) ans et doit être réexaminée au moins à la fin de cette échéance ou lors de chaque événement ou évolution de nature à modifier le contexte décrit dans le dossier d'homologation. Cette durée doit prendre en compte la sensibilité des risques résiduels, l'exposition du système d'information sensible aux nouvelles menaces, ainsi que les enjeux de sécurité du système d'information.

Lorsque l'urgence le requiert, une homologation provisoire peut être établie pour une durée de six (06) mois, renouvelable une seule fois. Ladite homologation provisoire doit être accompagnée d'un plan d'actions décrivant notamment les mesures de sécurité à mettre en place pour la maîtrise des risques.

3.4. Conditions de suspension ou de retrait de l'homologation

Durant la durée de l'homologation accordée, l'homologation reste valide tant que le système d'information est exploité dans le contexte décrit dans le dossier d'homologation.

Les changements, décrits ci-après, doivent impliquer un réexamen du dossier, pouvant conduire à une nouvelle décision d'homologation ou à un retrait de la décision :

- Raccordement d'un nouveau site sur le système d'information sensible ;
- Ajout d'une fonctionnalité majeure ;
- Succession de modifications mineures ;
- Réduction de l'effectif affecté à une tâche impactant la sécurité ;
- Changement d'un ou de plusieurs prestataires ;
- Non-respect d'au moins une des conditions de l'homologation ;
- Changement du niveau de sensibilité des informations traitées et, plus généralement, du niveau du risque ;
- Evolution du statut de l'homologation des systèmes interconnectés ;
- Publication d'incidents de nature à remettre en cause les garanties recueillies dans le dossier de sécurité.

4. Phase 4 : Suivi et maintien de l'homologation

Durant cette dernière phase, il est nécessaire de mettre en œuvre une procédure de révision périodique de l'homologation afin de s'assurer du respect des conditions de l'homologation et de revoir le répertoire des risques résiduels.

À ce titre, il est recommandé que l'équipe de l'homologation se réunisse régulièrement.

4.1. Suivi de l'homologation

À la suite de la décision d'homologation, l'équipe de l'homologation doit veiller au maintien du niveau de sécurité du système et à la réalisation annuelle du suivi de l'homologation. Ce suivi doit rester simple et se limiter à une mise à jour du dossier et à une analyse succincte des évolutions et des incidents intervenus au cours de l'année, afin de juger de l'opportunité d'une révision plus approfondie de l'homologation.

En préparation du renouvellement de l'homologation, le dossier d'homologation est régulièrement complété par les éventuelles analyses de vulnérabilités, les comptes rendus de contrôle et les rapports d'audits complémentaires.

4.2. Maintien en conditions de sécurité

Il est nécessaire que les conditions de l'homologation soient respectées dans le temps. À ce titre, l'équipe de l'homologation doit également assurer une veille technologique. Celle-ci permet d'identifier les vulnérabilités qui apparaîtraient sur le système et s'assurer qu'elles soient corrigées, notamment les plus sérieuses.

Annexe 1 : Description du système d'information sensible

Afin d'avoir une vision globale sur le fonctionnement, les interconnexions et les composants du système d'information sensible, les points suivantes permettent d'avoir une description complète de ce dernier :

- Objet et contexte d'utilisation du SIS ;
- Inventaire des actifs informationnels qui composent le SIS ;
- Interconnexion du SIS ;
- Architecture et cartographie réseau du SIS :
    - **La cartographie physique.** qui correspond à la répartition géographique des équipements et permet de connaître la position d'un équipement réseau au sein des différents sites ;
    - **La cartographie logique.** (plan d'adressage IP, noms de sous réseaux, liens logiques entre ceux-ci, principaux équipements actifs informationnels, etc.). Elle fait notamment apparaître les points d'interconnexion avec des entités « extérieures » (partenaires, fournisseurs de services, etc.) ainsi que l'ensemble des interconnexions avec Internet ;
    - **La cartographie des applications**. Le point de vue applicatif correspond aux applications métier et logiciels d'infrastructure utilisant l'architecture réseau comme support ;
    - **La cartographie de l'administration du système d'informations**. Elle représente le périmètre et le niveau de privilèges des administrateurs sur les ressources du parc informatique. Ce point de vue permet, en cas de compromission d'un compte d'administration, d'identifier le niveau de privilège de l'attaquant et la portion du parc potentiellement impactée.

Annexe 2 : Liste des documents pouvant être contenus dans le dossier d'homologation

Le dossier d'homologation peut contenir, en fonction de la complexité du système, les éléments suivants.

1. Le document de planification de l'homologation

C'est la feuille de route sur laquelle s'appuie l'ensemble des acteurs de l'homologation pour mener à bien la démarche d'homologation. C'est un document qui précise notamment :

- Une présentation générale du système ;
- Les acteurs de la démarche d'homologation ;
- Le périmètre de l'homologation ;
- Le planning de l'homologation ;
- Le coût estimé de la démarche d'homologation.

2. La politique de sécurité des systèmes d'information (PSSI)

La PSSI constitue le principal document de référence en matière de SSI d'une entité. C'est un plan d'actions qui vise à maintenir un certain niveau de sécurité et qui définit les objectifs à atteindre et les moyens accordés pour y parvenir.

3. Le journal de bord de l'homologation

Il s'agit du registre des décisions et des principaux événements qui sont intervenus pendant la démarche d'homologation. Il présente les caractéristiques suivantes :

- Il s'enrichit au fur et à mesure du projet (document de travail, feuille de route) pour adapter le processus aux évolutions du projet, notamment pour le planning ;
- Il permet de formaliser les prises de décisions et les mises au point nécessaires et de disposer d'un point de situation sur l'avancement de la démarche d'homologation (et les blocages éventuels).

4. Le rapport de l'analyse des risques et les objectifs de sécurité

Ce rapport doit être élaboré à l'issue de la gestion des risques de la phase 2 et présente les caractéristiques suivantes :

- Il décrit les besoins et objectifs de sécurité du système en termes de disponibilité, d'intégrité et de confidentialité par rapport aux menaces identifiées ;
- Il indique la nature et la sensibilité des informations traitées par le système et précise les contraintes qui restreignent la conception, l'exploitation et la maintenance du système.
- Il doit prendre en compte les architectures d'interconnexion, les moyens partagés avec d'autres entités, leurs conditions d'exploitation et de contrôle.
- Sa rédaction nécessite la participation des acteurs clés du système à homologuer, qui sont interrogés sur leurs besoins, le contexte d'emploi du système et les événements susceptibles d'impacter positivement ou négativement le système.

5. Le rapport d'audit de la sécurité du système d'information

Le rapport d'audit de la sécurité des systèmes d'information doit contenir en particulier :

- Une synthèse qui précise :
    - le contexte et le périmètre de la prestation ;

    - les vulnérabilités critiques, d'origine technique ou organisationnelle, et les mesures correctives proposées ;
    - l'appréciation du niveau de sécurité du système d'information audité par rapport à l'état de l'art et en considération du périmètre d'audit.
- Un tableau synthétique des résultats de l'audit, qui précise :
    - la synthèse des vulnérabilités relevées ;
    - la synthèse des mesures correctives proposées, classées par criticité et par complexité ou coût estimé de correction ;
- Lorsque réalisés, une description du déroulement des tests d'intrusion et de la méthodologie employée pour détecter les vulnérabilités et, le cas échéant, les exploiter.

6. Liste des mesures de sécurité appliquées aux systèmes d'information sensible

Cette liste énumère les moyens concrets pouvant être mis en œuvre pour assurer, partiellement ou totalement, la sécurité du système d'information sensible contre toute menace identifiée. Il convient de choisir les moyens nécessaires, suffisants, et justes qui peuvent être d'ordre technique, organisationnel, juridique ou humain.

7. Le répertoire des risques résiduels

Ce répertoire recense les risques résiduels en indiquant :

- Les raisons justifiant leur acceptation ;
- Leurs éventuelles vulnérabilités ;
- Leurs degrés de criticité ;
- L'échéance pour l'atténuation de leurs impacts ;
- Les actions potentielles pouvant les corriger.

8. Les procédures d'exploitation du système

Ces procédures doivent être détaillées et directement applicables. Elles exposent les mesures de sécurité permettant de répondre aux objectifs de sécurité fixés par les responsables de l'homologation. Elles présentent les droits et les devoirs des accédants au système d'information ainsi que les actions à réaliser dans le cadre de l'utilisation quotidienne dudit système.

9. Les attestations de qualification des produits ou prestataires

Dans la mesure où le système met en œuvre des produits de sécurité certifiés ou qualifiés ou encore des services de confiance qualifiés, il est nécessaire d'inclure les attestations correspondantes dans le dossier d'homologation.

Si elles sont disponibles, les analyses de sécurité des produits de sécurité, en particulier les instructions techniques d'emploi, peuvent également être intégrées au dossier d'homologation.

10. Le tableau de bord des incidents et de leurs résolutions

Ce tableau recueille l'ensemble des incidents survenus sur le SIS avec l'identification de leurs causes, leurs conséquences et les modalités de leurs résolutions.

11. Le plan de continuité/reprise d'activité (PCA/PRA)

Le PCA/PRA est un document qui met en œuvre un ensemble de procédure de protection permettant d'éviter certains événements, ou tout du moins d'en limiter les effets directs sur les objectifs de l'entité, et d'assurer les exigences métier habituelles malgré la perte de ressources critiques.

Annexe 3 : Liste des menaces

Le tableau suivant donne des exemples de menaces type. Cette liste peut être utilisée lors du processus d'appréciation des menaces. La liste suivante indique pour chaque type de menace si D (délibérée) pour les actions délibérées destinées aux actifs informationnels, A (accidentelle) pour toutes les actions humaines qui peuvent endommager les actifs informationnels de manière accidentelle, ou E (environnementale) pour tous les incidents qui ne reposent pas sur des actions humaines.

Type	Menaces	Origine
Dommage physique	Incendie	A, D, E
	Dégât des eaux	A, D, E
	Pollution	A, D, E
	Accident majeur	A, D, E
	Destruction de matériel ou de support	A, D, E
	Poussière, corrosion, congélation	A, D, E
Catastrophes naturelles	Phénomène climatique	E
	Phénomène sismique	E
	Phénomène volcanique	E
	Phénomène météorologique	E
	Inondation	E
Perte de services essentiels	Panne du système de climatisation ou d'alimentation en eau	A, D
	Perte de la source d'alimentation en électricité	A, D, E
	Panne du matériel de télécommunications	A, D
Perturbation due à des rayonnements	Rayonnements électromagnétiques	A, D, E
	Rayonnements thermiques	A, D, E
	Impulsions électromagnétiques	A, D, E
Compromission d'informations	Interception de signaux d'interférence compromettants	D
	Espionnage à distance	D
	Ecoute	D
	Vol de supports ou de documents	D
	Vol de matériel	D
	Récupération de supports recyclés ou mis au rebut	D
	Divulgation	A, D
	Données provenant de sources douteuses	A, D
	Piégeage de matériel	D
	Piégeage de logiciel	A, D
	Géolocalisation	D
Défaillances techniques	Panne de matériel	A
	Dysfonctionnement du matériel	A
	Saturation du système d'information	A, D
	Dysfonctionnement du logiciel	A
	Violation de la maintenabilité du système d'information	A, D
Actions non autorisées	Utilisation non autorisée du matériel	D
	Reproduction frauduleuse de logiciel	D
	Utilisation de logiciels copiés ou de contrefaçon	A, D

Type	Menaces	Origine
	Corruption de données	D
	Traitement illégal de données	D
Compromission des fonctions	Erreur d'utilisation	A
	Abus des droits	A, D
	Usurpation de droits	D
	Déni d'actions	D
	Violation de la disponibilité du personnel	A, D, E

Annexe 4 : Identification des actifs informationnels

Il est possible de distinguer les actifs informationnels de la manière suivante :

Types d'actifs	Sous types	Description
Actifs primordiaux : les processus centraux et informations de l'activité	• Processus	• Processus support et métier.
	• Informations	• Informations créées, traitées, stockées, archivées, etc. par l'entité.
Actifs en support : sur lesquels reposent les actifs primordiaux du domaine d'application	• Matériel	• Equipement de traitement des données (serveur, poste de travail fixe, ordinateur portable, etc.) • Périphériques de traitement (imprimante, lecteur de disque amovible…) • Support de données : Il s'agit de supports destinés à stocker des données ou des fonctions (CD ROM, cartouche de secours, disque dur amovible, clé USB, etc.), • Autres supports (papier, diapositive, etc.).
	• Logiciels	• Systèmes d'exploitation, • Applications métier ou supports.
	• Réseau	• Supports (Ethernet, VOIP, ADSL, spécifications de protocole sans fil (par exemple WiFi 802.11), etc.). • Relais actif ou passif (pont, switch, routeur, concentrateur, sélecteur, central automatique, etc.) • Interfaces de communication
	• Personnel	• Décideurs • RSSI • Développeurs • Personnel d'exploitation / de maintenance • Utilisateurs
	• Site	• Locaux de l'entité • Environnement extérieur (tous les emplacements au sein desquels les moyens de sécurité de l'entité ne peuvent s'appliquer). Exemples : résidence du personnel, locaux d'une autre entité, environnement situé à l'extérieur du site (zone urbaine, zone dangereuse). • Zone Une zone est formée par une limite physique de protection créant des cloisons dans les locaux d'une entité. Exemples : bureaux, zone d'accès réservé, zone sécurisée. • Services et moyens (sources et câblage) nécessaires pour alimenter le matériel et les périphériques de

		technologie de l'information (alimentation électrique basse tension, onduleur, appareil de climatisation, etc…).
	• Structure de l'entité	• Autorités (entité responsable, siège de l'entité). • Structure de l'entité (organigramme comprenant les différentes branches de l'entité) • Tiers (sous-traitants, fournisseurs, fabricants, etc…).

Annexe 5 : Modèle de la décision d'homologation

1. Contexte

Contexte d'homologation
Cadre réglementaire applicable

2. Présentation du SIS

Description du SIS
Enjeux et missions du SIS
Besoins de sécurité
Architecture du SI cible
Interconnexions
Sites de déploiement

3. Décision d'homologation

3.1. Homologation

Le « *fonction du responsable de l'IIV* », représentant « *dénomination de l'IIV* »

Décide

que le système d'information « *nom du SIS* » tel qu'il est décrit dans le dossier d'homologation « *référence du dossier d'homologation* » est homologué.

La présente décision d'homologation est valable à compter du « *jj/mm/aaaa* » jusqu'au « *jj/mm/aaaa* ».

La décision d'homologation reste valide tant que le système d'information est exploité dans le contexte décrit dans le dossier d'homologation « *référence du dossier d'homologation* ».

Cachet et signature

3.2. Homologation provisoire

Le « *fonction du responsable de l'IIV* », représentant « *dénomination de l'IIV* »

Considérant :

- Soit un aspect opérationnel ;
- Soit un risque accepté pour une durée limitée ;
- Soit un périmètre fonctionnel limité ;
- Soit un périmètre physique limité.

Décide

que le système d'information *« nom du SIS »* tel qu'il est décrit dans le dossier d'homologation *« référence du dossier d'homologation »* est homologué provisoirement et sous réserve de correction des faits constatés et précisés dans le plan d'actions, ci-joint à la présente décision d'homologation provisoire.

La présente décision d'homologation provisoire est valable à compter du *« jj/mm/aaaa »* jusqu'au *« jj/mm/aaaa ».*

La décision d'homologation provisoire reste valide tant que le système d'information est exploité dans le contexte décrit dans le dossier d'homologation *« référence du dossier d'homologation »*.

Cachet et signature