Cybersécurité et résilience des infrastructures critiques au Maroc : ce que doit la loi n° 05-20

Pr. Radouane Mrabet

AMSSNuR, Rabat, le 22 octobre 2025

2ème objectif de la loi 05-20

La loi 05-20 fixe les règles et les dispositions de sécurité applicables aux **infrastructures d'importance vitale**.

Les installations, les ouvrages et les systèmes qui sont indispensables au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social, et dont le dommage ou l'indisponibilité ou la destruction aurait un impact induisant la défaillance de ces fonctions.

Quelles sont les dispositions de la loi 05-20 propres aux infrastructures d'importance vitale disposant de systèmes d'information sensibles ?

Définition de « Système d'information sensible »

Système d'information traitant des informations ou des données sensibles sur lesquelles une atteinte à la confidentialité, à l'intégrité ou à la disponibilité porterait préjudice à une entité ou à une infrastructure d'importance vitale.

Référentiel de la classification des actifs informationnels et des systèmes d'information

Un **actif informationnel** consiste en toute ressource tel que le matériel, le logiciel, la donnée ou la procédure, qui composent les systèmes d'information

Selon l'article 10 du décret 2-21-406, les actifs informationnels et les systèmes d'information sont classifiés en fonction de **l'impact potentiel d'un incident de cybersécurité** sur les trois fonctions de base de la sécurité des systèmes d'information que sont **la confidentialité, la disponibilité et l'intégrité**.

Référentiel de la classification des actifs informationnels et des systèmes d'information

Conformément aux dispositions de l'article 10 susmentionné, la classification doit être effectuée en deux étapes :

Étape 1. chaque entité réalise une analyse des impacts des incidents de cybersécurité portant sur la confidentialité, la disponibilité ou l'intégrité de leurs actifs informationnels. L'échelle d'impact comporte quatre niveaux : « **très grave** », « **grave** », « **modéré** » et « **limité** ».

Référentiel de la classification des actifs informationnels et des systèmes d'information

Étape 2. classification des systèmes d'information sur la base de l'échelle de l'analyse des impacts prévue à l'article 11.

Les systèmes d'information sont classifiés en quatre niveaux, notés **A, B, C et D**. Le niveau A est le plus élevé, tandis que le niveau D est le moins élevé.

Référentiel de la classification des actifs informationnels et des systèmes d'information

Classe A → au moins un incident a un impact très grave

Classe B → tous les incidents ont au max un impact grave

Classe C → tous les incidents ont au max un impact modéré

Classe D → tous les incidents ont au max un impact limité

Sont réputés systèmes d'information sensibles, les systèmes d'information appartenant aux « Classe A » ou « Classe B ».

Quelles sont les dispositions de la loi 05-20 propres aux infrastructures d'importance vitale disposant de systèmes d'information sensibles ?

Dispositions de sécurité propres aux IIV

ART 14

Les articles 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 et 13 applicables aux IIV

ART 15

Fixer par décret la liste des secteurs d'activités d'importance vitale

ART 16

Lister par secteur d'activités d'importance vitale les IIV

ART 17 & 18

Etablir et tenir à jour la liste des SI sensibles par IIV

ART 19

Homologation des SI sensibles

ART 20 → 23

Audit des SI sensibles des IIV et transmission sécurisée du rapport d'audit à la DGSSI

ART 24

Elaboration et suivi régulier du plan d'action après audit

ART 25

Recours à des solutions de sécurité et des prestataires qualifiés pour le renforcement du dispositif

Dispositions de sécurité propres aux IIV

ART 14

Les articles 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 et 13 applicables aux IIV

L'article 14 de la loi 05-20 précise que les dispositions des articles 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 et 13 s'appliquent aux infrastructures d'importance vitale.

Dispositions de sécurité propres aux **entités**

ART 3

Mise en conformité aux directives et référentiels édictés par la DGSSI

ART 4

Mise en œuvre de la PSSI, cartographie des risques et réalisation des audits

ART 5

Classification des actifs informationnels et des SI

ART 6

Désignation d'un RSSI et assurer son indépendance

ART 7

Mise en place de solutions de détection et de supervision des événements

ART 8

Mise en place du processus de gestion des incidents et de signalement des évènements

ART 9

Elaboration d'un plan de continuité d'activités et assurer son test régulier

ART 10 → 13

Mise en place d'une politique d'externalisation des SI sensibles et leurs hébergements au Maroc

Dispositions de sécurité propres aux IIV

ART 15

Fixer par décret la liste des secteurs d'activités d'importance vitale

ART 16

Lister par secteur d'activités d'importance vitale les IIV

ART 17 & 18

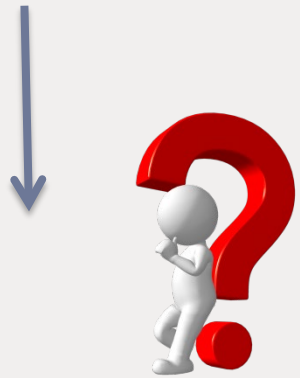
Etablir et tenir à jour la liste des SI sensibles par IIV

Définition de « Secteur d'activités d'importance vitale »

L'ensemble des activités exercées par les infrastructures d'importance vitale et concourant à un même objectif. Ces activités ont trait soit à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, ou à l'exercice des prérogatives de l'Etat ou au maintien de ses capacités de sécurité ou au fonctionnement de l'économie, dès lors que ces activités sont difficilement substituables ou remplaçables, ou qui peuvent présenter un danger grave pour la population.

Dispositions propres aux IIV – liste des secteurs d'activités d'importance vitale

Article 15 : La liste des secteurs d'activités d'importance vitale et des autorités gouvernementales, établissements publics ou autres personnes morales de droit public, assurant la coordination de ces secteurs est fixée par voie réglementaire.



Annexe 1 du décret n° 2-21-406

ANNEXE 1

Liste des secteurs d'activités d'importance vitale et les autorités gouvernementales, établissements publics et personnes morales de droit public, assurant la coordination de ces secteurs

Secteurs d'activités d'importance vitale	**Autorités gouvernementales, établissements publics et personnes morales de droit public, assurant la coordination de ces secteurs**
Secteur de la sécurité publique	Autorité gouvernementale chargée de l'intérieur
Secteur des affaires étrangères	Autorité gouvernementale chargée des affaires étrangères
Secteur des finances	Autorité gouvernementale chargée des finances
Secteur de la législation	Secrétariat général du gouvernement
Secteur de l'agriculture	Autorité gouvernementale chargée de l'agriculture
Secteur de la santé	Autorité gouvernementale chargée de la santé
Secteurs de l'industrie, du commerce et de l'économie numérique	Autorité gouvernementale chargée de l'industrie, du commerce et de l'économie numérique

Secteur de la communication audiovisuelle	Autorité gouvernementale chargée de la communication
Secteur de la production et de la distribution de l'énergie	Autorité gouvernementale chargée de l'intérieur
	Autorité gouvernementale chargée de l'énergie
Secteur des mines	Autorité gouvernementale chargée des mines
Secteur des transports	Autorités gouvernementales chargées des transports
Secteur de la production et de la distribution d'eau	Autorités gouvernementales chargées de l'eau
Secteur bancaire	Bank Al-Maghrib
Secteur des télécommunications	Agence nationale de réglementation des télécommunications
Secteur des assurances et de la prévoyance sociale	Autorité de contrôle des assurances et de la prévoyance sociale

Secteur de la communication audiovisuelle	Autorité gouvernementale chargée de la communication
Secteur de la production et de la distribution de l'énergie	Autorité gouvernementale chargée de l'intérieur
	Autorité gouvernementale chargée de l'énergie
Secteur des mines	Autorité gouvernementale chargée des mines
Secteur des transports	Autorités gouvernementales chargées des transports
Secteur de la production et de la distribution d'eau	Autorités gouvernementales chargées de l'eau
Secteur bancaire	Bank Al-Maghrib
Secteur des télécommunications	Agence nationale de réglementation des télécommunications
Secteur des assurances et de la prévoyance sociale	Autorité de contrôle des assurances et de la prévoyance sociale

Dispositions de sécurité propres aux IIV

ART 15

Fixer par décret la liste des secteurs d'activités d'importance vitale

ART 16

Lister par secteur d'activités d'importance vitale les IIV

ART 17 & 18

Etablir et tenir à jour la liste des SI sensibles par IIV

Dispositions propres aux IIV – liste des infrastructures d'importance vitale

Article 16 : Les infrastructures d'importance vitale sont désignées pour chaque secteur d'activité d'importance vitale par l'autorité gouvernementale, l'établissement public ou la personne morale de droit public dont relève la coordination de ce secteur, et ce après avis de l'autorité nationale.

La **liste de ces infrastructures doit être tenue secrète** et doit être actualisée à intervalles réguliers et au moins tous les deux ans.

Dispositio
infrastruc

Article 16 : Le
chaque secte
gouvernementa
public dont re
l'autorité nationale.

- Chaque secteur d'activité a la responsabilité de désigner ses propres infrastructures d'importance vitale.
- La désignation des IIV est une responsabilité importante qui doit être effectuée avec soin même si les critères à utiliser pour désigner les IIV ne sont pas précisés.
- La DGSSI donne son avis dans le processus de désignation afin qu'elle assure une approche cohérente et harmonisée sur le territoire nationale.
- La confidentialité de la liste des IIV est essentielle pour protéger ces systèmes contre les attaques ciblées.

La **liste de ces infrastructures doit être tenue secrète** et doit être actualisée à intervalles réguliers et au moins tous les deux ans.

Dispositions de sécurité propres aux IIV

ART 15

Fixer par décret la liste des secteurs d'activités d'importance vitale

ART 16

Lister par secteur d'activités d'importance vitale les IIV

ART 17 & 18

Etablir et tenir à jour la liste des SI sensibles par IIV

Dispositions propres aux IIV – liste des systèmes d'information sensibles

Article 17 : Le responsable de l'infrastructure d'importance vitale établit, sur la base des résultats d'une analyse des risques, la liste des systèmes d'information sensibles et la transmet avec les mises à jour de celle-ci à l'autorité nationale.

Dispositions propres aux IIV – liste des systèmes d'information sensibles

Article 18 : L'autorité nationale peut faire des observations au responsable de l'infrastructure d'importance vitale sur la liste des systèmes d'information sensibles qui lui a été transmise.

Dans ce cas, le responsable de l'infrastructure d'importance vitale est tenu de modifier sa liste conformément à ces observations et transmet la liste modifiée à l'autorité nationale dans un délai de deux mois à compter de la date de réception des observations.

La liste des systèmes d'information sensibles doit être tenue secrète.

Dispositio
d'informat

Article 18 : L'au

l'infrastructure d'i

lui a été transmise

Dans ce cas, le res

sa liste conformément à ces observations et transmet la liste modifiée à l'autorité nationale dans un délai de deux mois à compter de la date de réception des observations.

- L'article 18 joue un rôle clé dans la collaboration et la coordination entre l'autorité nationale et les responsables de l'IIV concernant la liste des SIS.
- En permettant à la DGSSI de faire des observations et en obligeant le responsable de l'IIV à ajuster sa liste en conséquence, cette disposition garantit que la liste des SIS est complète, précise et à jour, reflétant ainsi les risques et menaces réels auxquels l'IIV est confrontée.

La liste des systèmes d'information sensibles doit être tenue secrète.

Dispositions de sécurité propres aux IIV

ART 19

Homologation des SI sensibles

13. Définition de « Homologation des systèmes d'information »

Document par lequel le responsable d'une infrastructure d'importance vitale atteste de sa connaissance du système d'information et des mesures de sécurité techniques, organisationnelles ou juridiques mises en œuvre et accepte les risques résiduels.

Dispositions propres aux IIV – Homologation de la sécurité d'un système d'information sensible

- Les articles 16, 17 et 18 permettent d'identifier les SIS qui se trouvent dans les IIV. Cette étape d'identification est importante mais non suffisante pour les sécuriser et les rendre résilients aux cyberattaques.
- Le législateur a prévu une deuxième étape excessivement importante qu'est l'homologation. C'est une étape assez longue, complexe et couteuse que le responsable du SIS doit mener pour atteindre un niveau de sécurité satisfaisant.

Dispositions propres aux IIV – Homologation de la sécurité d'un système d'information sensible

- L'homologation vise à évaluer et à certifier que les mesures de sécurité mises en place pour protéger un SIS sont conformes aux normes et aux exigences de sécurité applicables.
- Elle permet de garantir que les SIS sont suffisamment protégés contre les cybermenaces et les vulnérabilités, et qu'ils respectent les exigences légales et réglementaires en matière de sécurité de l'information.

Dispositions propres aux IIV – Homologation de la sécurité d'un système d'information sensible

Article 19 : Tout système d'information sensible doit faire l'objet d'une homologation de sa sécurité avant sa mise en exploitation.

Le guide d'homologation des systèmes d'information sensibles est fixé par l'autorité nationale.

Ce guide est disponible sur le site de la DGSSI

Dispositions de sécurité propres aux IIV

ART 20 → 23

Audit des SI sensibles des IIV et transmission sécurisée du rapport d'audit à la DGSSI

ART 24

Elaboration et suivi régulier du plan d'action après audit

Loi n° 05-20 - article 4 alinéas 3 et 4 :

Tout système d'information d'une entité offrant des services numériques à des tiers doit, avant sa mise en exploitation, faire l'objet d'un audit de sa sécurité.

Chaque entité doit, régulièrement, auditer ses systèmes d'information.

ART 20 → 23

Audit des SI sensibles des IIV et transmission sécurisée du rapport d'audit à la DGSSI

ART 24

Elaboration et suivi régulier du plan d'action après audit

Dispositions propres aux IIV – liste des systèmes d'information sensibles

Article 20 : A la demande de l'autorité nationale, les responsables des infrastructures d'importance vitale soumettent les systèmes d'information sensibles desdites infrastructures à un **audit** effectué par cette autorité ou par des prestataires d'audit qualifiés par ladite autorité.

Les critères de qualification des prestataires d'audit et les modalités de déroulement de l'audit sont fixés par voie réglementaire.

Décret n° 2-21-406 du 15 juillet 2021

Liste des prestataires d'audit de la sécurité des systèmes d'information qualifiés (20/10/2025)

Prestataire	Audit Organisationnel et Physique	Audit d'Architecture	Audit de configuration	Tests d'intrusion	Audit du code source	Audit des systèmes industriels	Date de fin de qualification	Classe des SI	Décision de qualification
Entreprise Services CDG (DXC Technology)	✓	✓	✓	✓			17/07/2028	Classe B	PDF
LMPS CONSULTING	✓	✓	✓	✓	✓	✓	02/02/2027	Classe B	PDF
Deloitte Morocco Cyber Center	✓	✓	✓	✓	✓	✓	03/11/2026	Classe B	PDF
Techso Group	✓	✓	✓	✓	✓	✓	18/08/2026	Classe B	PDF
SEKERA SERVICES	✓	✓	✓	✓	✓		18/08/2026	Classe A et Classe B	PDF
NEAR SECURE	✓	✓	✓	✓	✓	✓	18/08/2026	Classe A et Classe B	PDF
DATAPROTECT	✓	✓	✓	✓	✓	✓	17/01/2026	Classe A et Classe B	PDF
PWC Advisory	✓		✓	✓			12/01/2026	Classe B	PDF

Domaines d'audit de sécurité

Annexe 2 du décret n° 2-21-406 pris pour l'application de la loi n° 05-20 :

Domaines d'audit objet de la qualification des prestataires d'audit de la sécurité des systèmes d'information

- **audit organisationnel et physique** : consiste à s'assurer que les politiques et procédures de sécurité définies et mises en place par l'entité auditée sont conformes aux directives de l'autorité nationale ;
- **audit d'architecture** : consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information, aux pratiques en vigueur, aux exigences de sécurité et aux règles internes de l'entité auditée ;
- **audit de configuration** : permet de vérifier la mise en œuvre de pratiques de sécurité conformes aux exigences et règles internes de l'entité auditée en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information ;
- **audit de code source** : consiste en l'analyse de tout ou partie du code source ou des conditions de compilation d'une solution logicielle dans le but de s'assurer du respect des règles précises du codage ou d'analyser les vulnérabilités liées au développement ;
- **test d'intrusion** : permet d'évaluer la sécurité d'un système d'information ou d'un réseau en simulant les conditions réelles d'une attaque sur le système d'information. Ce test permet de découvrir des vulnérabilités sur le système d'information d'une entité auditée et de vérifier leur exploitabilité et leur impact sur l'entité ;
- **audit des systèmes industriels** : consiste en l'évaluation du niveau de sécurité d'un système industriel et des dispositifs de contrôle associés.

Dispositions de sécurité propres aux IIV

ART 20 → 23

Audit des SI sensibles des IIV et transmission sécurisée du rapport d'audit à la DGSSI

ART 24

Elaboration et suivi régulier du plan d'action après audit

Dispositions propres aux IIV – Plan d'actions après audit

Article 24 : Chaque responsable d'infrastructure d'importance vitale auditée doit mettre en place un plan d'actions pour mettre en œuvre les recommandations figurant dans les rapports d'audit et le transmet à l'autorité nationale pour le suivi de sa mise en œuvre.

Dispositions de sécurité propres aux IIV

ART 25

Recours à des solutions de sécurité et des prestataires qualifiés pour le renforcement du dispositif

Dispositions propres aux IIV – Utilisation de services, produits et solutions pour renforcer les fonctions de sécurité

Article 25 alinéa 1 : Les responsables des infrastructures d'importance vitale doivent recourir à des services, produits ou solutions qui permettent le renforcement des fonctions de sécurité, définis par l'autorité nationale.

Dispositions propres aux IIV – Utilisation de services, produits et solutions pour renforcer les fonctions de sécurité

Article 25 alinéa 1 : Les responsables des infrastructures d'importance vitale doivent recourir à

le renforcement des fon

ARTICLE PREMIER. – Pour l'application des dispositions du premier alinéa de l'article 25 de la loi susvisée n° 05-20, les responsables des entités et des infrastructures d'importance vitale doivent, lorsqu'ils recourent à des services Cloud en ce qui concerne les systèmes d'information sensibles et les données sensibles, notamment pour renforcer leurs fonctions de sécurité, faire appel à un prestataire de services Cloud qualifié, conformément aux dispositions du présent décret.

Dispositions de sécurité propres aux IIV

ART 14

Les articles 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 et 13 applicables aux IIV

ART 15

Fixer par décret la liste des secteurs d'activités d'importance vitale

ART 16

Lister par secteur d'activités d'importance vitale les IIV

ART 17 & 18

Etablir et tenir à jour la liste des SI sensibles par IIV

ART 19

Homologation des SI sensibles

ART 20 → 23

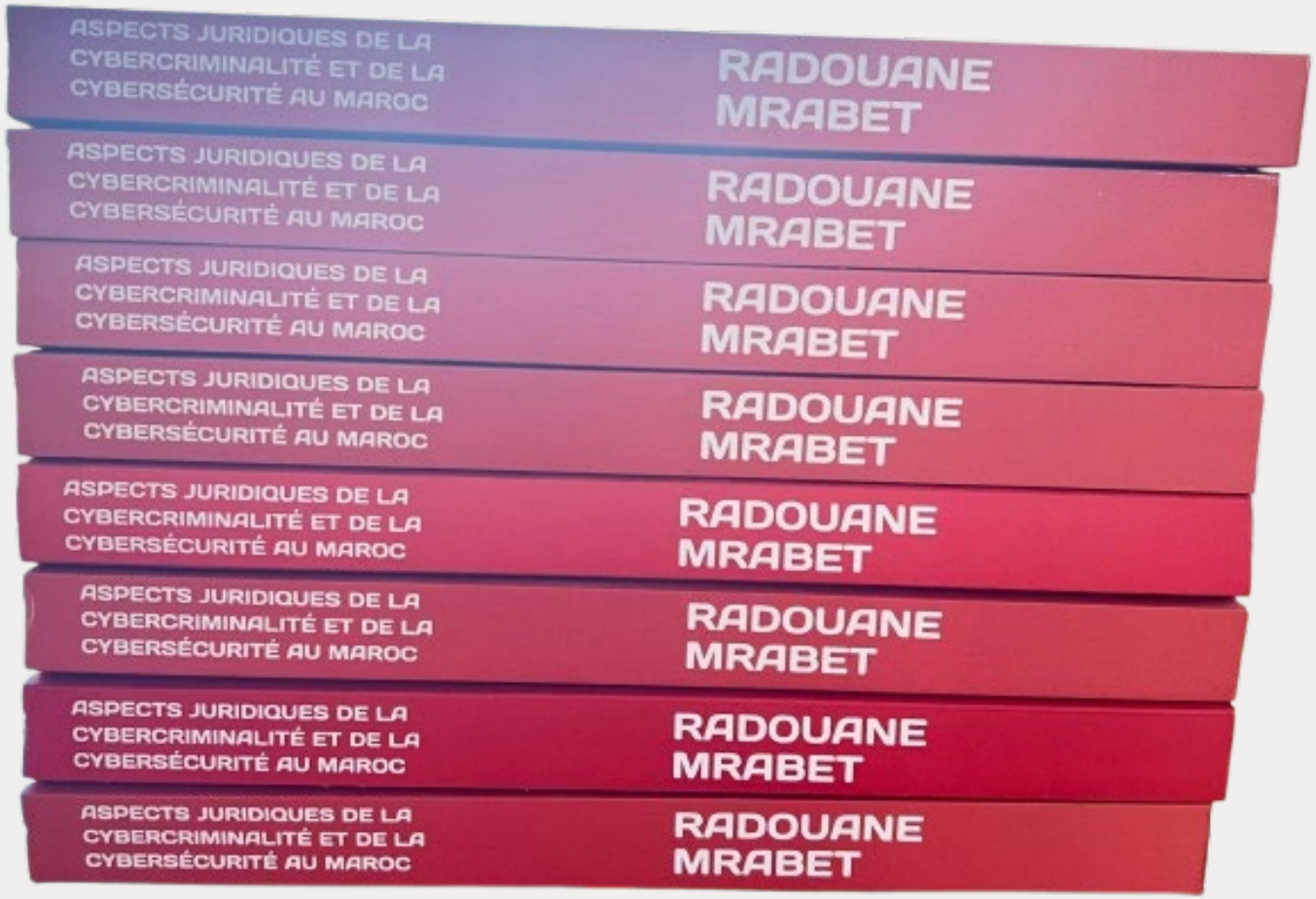
Audit des SI sensibles des IIV et transmission sécurisée du rapport d'audit à la DGSSI

ART 24

Elaboration et suivi régulier du plan d'action après audit

ART 25

Recours à des solutions de sécurité et des prestataires qualifiés pour le renforcement du dispositif



amazon https://www.amazon.fr/dp/B0DLTL343G

Merci pour votre attention

Pr. Radouane Mrabet

ENSIAS, Université Mohammed V de Rabat

AMSSNuR, Rabat,
le 22 octobre 2025