Cybersecurity and resilience of critical infrastructure in Morocco:

What Law No. 05-20 must address?

Pr. Radouane Mrabet

AMSSNuR, Rabat, le 22th October 2025

2nd objective of law 05-20

Law 05-20 establishes the rules and security provisions applicable to **vital infrastructure**.

The facilities, structures, and systems that are essential for maintaining the vital functions of society, health, safety, security, and economic or social well-being, and whose damage, unavailability, or destruction would have an impact leading to the failure of these functions.

What are the specific provisions of Law 05-20 concerning critical infrastructure with sensitive information systems?

Definition of "Sensitive Information System"

Information system processing sensitive information or data where a breach of confidentiality, integrity or availability would harm a critical entity or infrastructure.

Reference framework for the classification of information assets and information systems

An **information asset** consists of any resource, such as hardware, software, data, or procedures, that make up information systems

According to **Article 10 of Decree 2-21-406**, information assets and information systems are classified according to the **potential impact of a cybersecurity incident** on the three basic functions of information systems security: **confidentiality, availability, and integrity**.

Reference framework for the classification of information assets and information systems

In accordance with the provisions of Article 10 above, the classification must be carried out in two stages:

Stage 1. Each entity conducts an impact analysis of cybersecurity incidents affecting the confidentiality, availability, or integrity of its information assets. The impact scale comprises four levels: "**very severe**," "**severe**," "**moderate**," and "**limited**."

Reference framework for the classification of information assets and information systems

Stage 2. Classification of information systems based on the impact assessment scale provided for in Article 11.Information systems are classified into four levels, labeled **A**, **B**, **C**, and **D**. Level A is the highest, while level D is the lowest.

Reference framework for the classification of information assets and information systems

Class A → at least one incident has a very serious impact.

Class B → all incidents have a maximum serious impact.

Class C → all incidents have a maximum moderate impact.

Class D → all incidents have a maximum limited impact.

Information systems are considered sensitive if they belong to "Class A" or "Class B".

What are the specific provisions of Law 05-20 concerning critical infrastructure with sensitive information systems?

Security provisions specific to IIVs

ART 14

Articles 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 and 13 applicable to IV

ART 15

Establish by decree the list of sectors of vital importance

ART 16

List by sector of vital importance the IIVs

ART 17 & 18

Establish and maintain the list of sensitive information systems by IV

ART 19

Approval of sensitive information systems

ART 20 → 23

Auditing sensitive IT systems of the IIVs and securely transmitting the audit report to the DGSSI

ART 24

Development and regular monitoring of the action plan following the audit

ART 25

Use of security solutions and qualified service providers to strengthen the system

Security provisions specific to IIVs

ART 14

Articles 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 and 13 applicable to IV

Article **14** of Law 05-20 specifies that the provisions of Articles 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 and 13 apply to vital infrastructure.

Security provisions specific to entities

ART 3

Compliance with the directives and standards issued by the DGSSI

ART 4

Implementation of the Information Systems Security Policy (ISSP), risk mapping and execution of audits

ART 5

Classification of information assets and information systems

ART 6

Appointing a RSSI and ensuring their independence

ART 7

Implementation of event detection and monitoring solutions

ART 8

Implementation of the incident management and event reporting process

ART 9

Developing a business continuity plan and ensuring its regular testing

ART 10 → 13

Implementation of a policy for outsourcing sensitive IT systems and their hosting in Morocco

Security provisions specific to IIVs

ART 15

Establish by decree the list of sectors of vital importance

ART 16

List by sector of vital importance the IIVs

ART 17 & 18

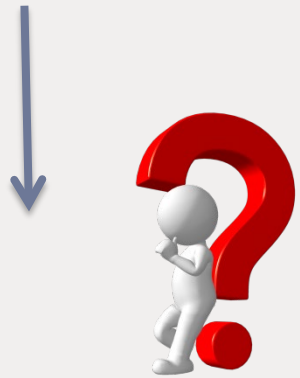
Establish and maintain the list of sensitive information systems by IV

Definition of "Sector of vital importance"

All activities carried out by vital infrastructure and contributing to the same objective. These activities relate either to the production and distribution of goods or services essential to meeting the basic needs of the population, or to the exercise of state prerogatives, the maintenance of its security capabilities, or the functioning of the economy, insofar as these activities are difficult to substitute or replace, or may present a serious danger to the population.

Specific provisions for IIV – list of sectors of vital importance

Article 15: The list of sectors of vital importance and of the government authorities, public institutions or other legal entities under public law, ensuring the coordination of these sectors, **shall be established by regulation**.



Annex 1 of Decree No. 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

Security provisions specific to IIVs

ART 15

Establish by decree the list of sectors of vital importance

ART 16

List by sector of vital importance the IIVs

ART 17 & 18

Establish and maintain the list of sensitive information systems by IV

Specific provisions for IIV – list of vital infrastructure

Article 16: Critical infrastructure is designated for each critical sector of activity by the government authority, public institution, or public legal entity responsible for coordinating that sector, after consultation with the national authority.

The **list of this infrastructure must be kept confidential** and updated regularly, at least every two years.

Specific pr
infrastruct

- Each sector of activity is responsible for designating its own critical infrastructure.
- Designating critical infrastructure is an important responsibility that must be carried out carefully, even though the criteria for designating critical infrastructure are not specified.
- The DGSSI (General Directorate of Information Systems Security) provides input during the designation process to ensure a consistent and harmonized approach across the country.
- Maintaining the confidentiality of the critical infrastructure list is essential to protect these systems against targeted attacks..

Article 16: Crit

activity by the

entity responsil

national author

The **list of this infrastructure must be kept confidential** and updated regularly, at least every two years.

Security provisions specific to IIVs

ART 15

Establish by decree the list of sectors of vital importance

ART 16

List by sector of vital importance the IIVs

ART 17 & 18

Establish and maintain the list of sensitive information systems by IV

Specific provisions for IIVs – list of sensitive information systems

Article 17: The person responsible for the critical infrastructure shall establish, on the basis of the results of a risk analysis, the list of sensitive information systems and shall transmit it, along with updates thereof, to the national authority.

Specific provisions for IIVs – list of sensitive information systems

Article 18: The national authority may submit comments to the operator of the critical infrastructure regarding the list of sensitive information systems provided to it.

In this case, the operator of the critical infrastructure is required to amend the list in accordance with these comments and submit the amended list to the national authority within two months of receiving the comments.

The list of sensitive information systems must be kept confidential.

Specific pr
informatio

Article 18: The na

infrastructure rega

In this case, the c

accordance with

authority within tw

- Article 18 plays a key role in collaboration and coordination between the national authority and the IIV officials regarding the list of SIS.
- By allowing the DGSSI to submit comments and requiring the IIV official to adjust their list accordingly, this provision ensures that the SIS list is complete, accurate, and up-to-date, thus reflecting the actual risks and threats facing the IIV.

The list of sensitive information systems must be kept confidential.

Security provisions specific to IIVs

ART 19

Approval of sensitive information systems

13. Definition of “Information System Approval”

Document by which the person in charge of a critical infrastructure attests to their knowledge of the information system and the technical, organizational or legal security measures implemented and accepts the residual risks.

Specific provisions for IIV – Approval of the security of a sensitive information system

- Articles 16, 17, and 18 allow for the identification of Information Systems (ISS) located in the IIVs (Integrated Information Systems). This identification step is important but not sufficient to secure them and make them resilient to cyberattacks.
- The legislator has provided for a second, extremely important step: certification. This is a rather lengthy, complex, and costly process that the ISS manager must undertake to achieve a satisfactory level of security.

Specific provisions for IIV – Approval of the security of a sensitive information system

- Accreditation aims to assess and certify that the security measures implemented to protect a Information System (ISS) comply with applicable security standards and requirements.
- It ensures that ISSs are adequately protected against cyber threats and vulnerabilities, and that they meet legal and regulatory requirements for information security.

Specific provisions for IIV – Approval of the security of a sensitive information system

Article 19: All sensitive information systems must undergo security certification before being put into operation.

The certification guidelines for sensitive information systems are established by the national authority.

This guide is available on the DGSSI website

Security provisions specific to IIVs

ART 20 → 23

Auditing sensitive IT systems of the IIVs and securely transmitting the audit report to the DGSSI

ART 24

Development and regular monitoring of the action plan following the audit

Law No. 05-20, Article 4, paragraphs 3 and 4:

Each information system of an entity offering digital services to third parties must undergo a security audit before being put into operation.

Each entity must regularly audit its information systems.

ART 20 → 23

Auditing sensitive IT systems of the IIVs and securely transmitting the audit report to the DGSSI

ART 24

Development and regular monitoring of the action plan following the audit

Specific provisions for IIVs – list of sensitive information systems

Article 20: At the request of the national authority, those responsible for critical infrastructure shall submit the sensitive information systems of said infrastructure to an **audit** conducted by that authority or by audit providers qualified by that authority. The criteria for qualifying audit providers and the procedures for conducting the audit shall be established by regulation.

Decree No. 2-21-406 of July 15, 2021

List of qualified information systems security audit providers (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

Areas of security auditing

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.

Security provisions specific to IIVs

ART 20 → 23

Auditing sensitive IT systems of the IIVs and securely transmitting the audit report to the DGSSI

ART 24

Development and regular monitoring of the action plan following the audit

Specific provisions for IIVs – Post-audit action plan

Article 24: Each manager of critical infrastructure audited must put in place an action plan to implement the recommendations contained in the audit reports and transmit it to the national authority for monitoring of its implementation.

Security provisions specific to IIVs

ART 25

Use of security solutions and qualified service providers to strengthen the system.

Provisions specific to IIV – Use of services, products and solutions to enhance security functions

Article 25, paragraph 1: Those responsible for critical infrastructure must use services, products or solutions that enhance security functions, as defined by the national authority.

Provisions specific to IIV – Use of services, products and solutions to enhance security functions

Article 25, paragraph 1: The responsible for critical infrastructure must use services, products or solutions that enhance security functions, as defined by the national authority.

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.

Security provisions specific to IIVs

ART 14

Articles 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 and 13 applicable to IIV

ART 15

Establish by decree the list of sectors of vital importance

ART 16

List by sector of vital importance the IIVs

ART 17 & 18

Establish and maintain the list of sensitive information systems by IIV

ART 19

Approval of sensitive information systems

ART 20 → 23

Auditing sensitive IT systems of the IIVs and securely transmitting the audit report to the DGSSI

ART 24

Development and regular monitoring of the action plan following the audit

ART 25

Use of security solutions and qualified service providers to strengthen the system

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