ANSSI
Implementation of the NIS Directive in the French maritime sector

Sylvie ANDRAUD
sylvie.andraud@ssi.gouv.fr

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Introduction to ANSSI

2009: Creation of ANSSI

> The ***Agence Nationale de la Sécurité des Systèmes d'Information*** (ANSSI) was created on July 7th 2009 by a decree (2009-834) of the Prime Minister, which defines precisely its **authority** and **missions**.

> ANSSI is a service with **national responsibility**, which reports to the General Secretary for Defense and National Security.

> The decree (2011-170) of February 11th 2011 has appointed ANSSI **the French Cyberdefense authority**.

> ANSSI has 3 main missions: **prevention ; defense ; cooperation & promotion**

Our missions

> Targeted audience

- **Mainly**
  - ○ **Government infrastructures**
  - ○ **Critical and essential private or public operators for the country (OES = Operator of Essential Services ; OIV = Operator of Vital Importance, concerned by the Critical Information Infrastructure Protection (CIIP) law)**
- **Extending to non essential / non critical operators and the citizens**

> Scope of action

Defense

> Operational security (CERT-FR) :
- Vulnerability watch
- Protection & surveillance of certain state IS
- Dealing with incidents (State & OIV & OES)

> Supporting operations (State & OIV & OES)

> In charge of managing the response to any serious cyber attack against France.

Influence, cooperate and promote

> Producing regulatory directives (e.g. : transposition of the NIS directive in French law)

> Stakeholder within international negotiations in close relationship with other states counterparts

Prevention

> Define the rules of protection for critical information systems

> Support and assist the administration and critical infrastructure operators

> Prevent the threat by studying the different modes of attack

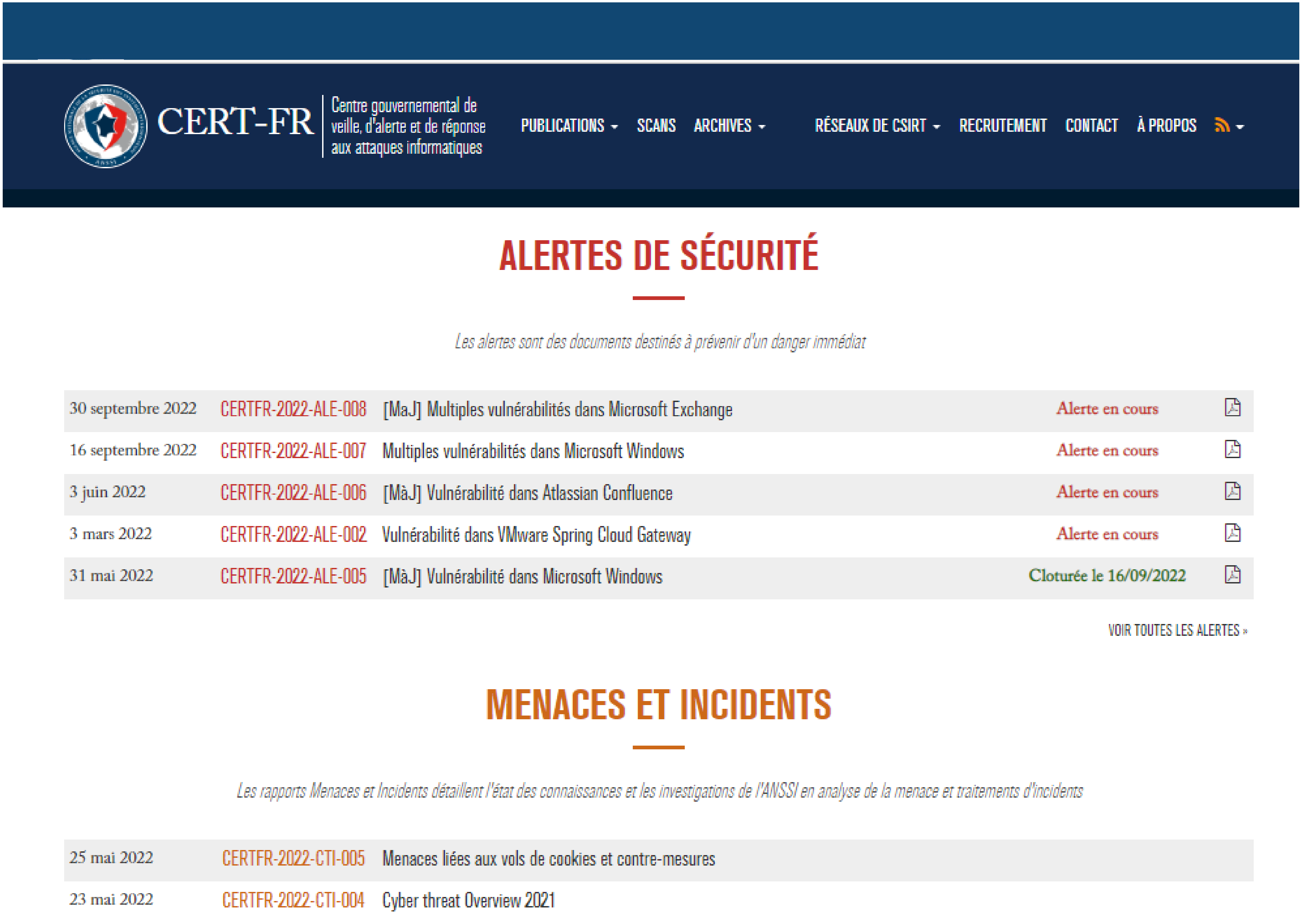
> Expertise, R&D, technology watch, maintained at "state of art" level

> Certification & qualification of IT products and services

> Inspections & audits (State & OIV & OES)

> Training, awareness & recommendation
- Guides, Best practices, MOOC
- Technical notes & recommandations

> Specific services : Microsoft AD security analysis (ADS), level of exposure on Internet (SILENE)


CERT-FR
Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques
PUBLICATIONS ▾
SCANS
ARCHIVES ▾
RÉSEAUX DE CSIRT ▾
RECRUTEMENT
CONTACT
À PROPOS

ALERTES DE SÉCURITÉ

Les alertes sont des documents destinés à prévenir d'un danger immédiat

30 septembre 2022	CERTFR-2022-ALE-008	[MaJ] Multiples vulnérabilités dans Microsoft Exchange	Alerte en cours	📄
16 septembre 2022	CERTFR-2022-ALE-007	Multiples vulnérabilités dans Microsoft Windows	Alerte en cours	📄
3 juin 2022	CERTFR-2022-ALE-006	[MàJ] Vulnérabilité dans Atlassian Confluence	Alerte en cours	📄
3 mars 2022	CERTFR-2022-ALE-002	Vulnérabilité dans VMware Spring Cloud Gateway	Alerte en cours	📄
31 mai 2022	CERTFR-2022-ALE-005	[MàJ] Vulnérabilité dans Microsoft Windows	Cloturée le 16/09/2022	📄

VOIR TOUTES LES ALERTES »

MENACES ET INCIDENTS

Les rapports Menaces et Incidents détaillent l'état des connaissances et les investigations de l'ANSSI en analyse de la menace et traitements d'incidents

25 mai 2022	CERTFR-2022-CTI-005	Menaces liées aux vols de cookies et contre-mesures
23 mai 2022	CERTFR-2022-CTI-004	Cyber threat Overview 2021

NIS Directive

2016, 6th of July: adoption by European institutions of Network and Information System Security Directive

NIS : a harmonised approach for member states (MS)

STRATÉGIE NATIONALE
POUR LA SÉCURITÉ
DU NUMÉRIQUE

- Obligations for all MS to :
  - adopt a national strategy on the security of network and information systems
  - Designate national competent authorities, single points of contact and CSIRTs
- Building cooperation at EU level :
  - the NIS Cooperation group
  - the computer security incident response team network (CSIRT network)
- Security and notification requirements for operators of essential services and for digital service providers

ANSSI is the French national authority, the single point of contact and the national CSIRT

The French Implementation of NIS DIrective

Mandatory transposition in national law

1 law	NIS directive transposition law *[Loi n°2018-133 du 26 février 2018]*
1 application decree	OES designation terms, EIS declaration terms, incident declaration terms, control terms, list of essential services *[Décret n° 2018-384 du 23 mai 2018]*
3 orders	1. Essential information system (EIS) declaration terms & incident declaration terms *[Arrêté du 13 juin 2018]* 2. Cost of controls *[Arrêté du 1er août 2018]* 3. Security rules & time limits for implementation *[Arrêté du 14 septembre 2018]*

https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/nis-un-dispositif-de-cybersecurite-pour-les-operateurs-de-service-essentiel/

The French Implementation of NIS DIrective

The law provides with 3 set of measures :

Security Requirements

A set of 23 technical and organisational rules is imposed to operators of essential services (OES)

Incidents notification

ANSSI is notified directly by operators of incidents occuring on their essential information systems.

Controls

ANSSI can trigger security audits led by itself or a Trust service provider.

The French Implementation of NIS DIrective

[Décret n° 2018-384 du 23 mai 2018]

- Each OES is designated by the Prime Minister (after coordination between the operator, ANSSI and the sectoral ministry) ; The designation order mentions the list of essential services provided by the OES
- In case of an essential service provided in other MS, the MS are consulted by ANSSI
- Each OES identifies and sends to ANSSI the list of its essential information systems (EIS), based on a risk analysis ; this list includes EIS managed by a third party
- Once a year, each OES sends to ANSSI the updates of its EIS list
- The decree provides the list of essential services (France has made the choice to add sectors to the list provided by the text of the 2016 directive)

[Arrêté du 14 septembre 2018 – Annexe II]

- Security measures, to be applied within 1 to 3 years

The French Implementation of NIS DIrective

[Arrêté du 13 juin 2018]

> ANSSI provides :

- An EIS reporting form, to be completed for each EIS
- an incident reporting form, to be completed in case of incident

[Arrêté du 1er août 2018]

> In case of a control, the OES has to pay the time spent by the auditors and the cost is determined by law

Be a French OES: First Implementation Steps

- Identification date + 2 months:

  The OES declares a representative to ANSSI

- Designation date + 3 months :

  The OES declares its EIS list to ANSSI

- As soon as the EIS are declared :

  The OES declares to ANSSI incidents having an impact on EIS

- Security measures : to be applied within 1 to 3 years

Trusted Service Providers

Different types of Trusted Service Providers :

- Cybersecurity audit service providers (PASSI)
- Incident detection service providers (PDIS)
- Incident response service providers (PRIS)
- Cloud providers (SecNumCloud)
- Secured administration and maintenance service providers (PAMS)

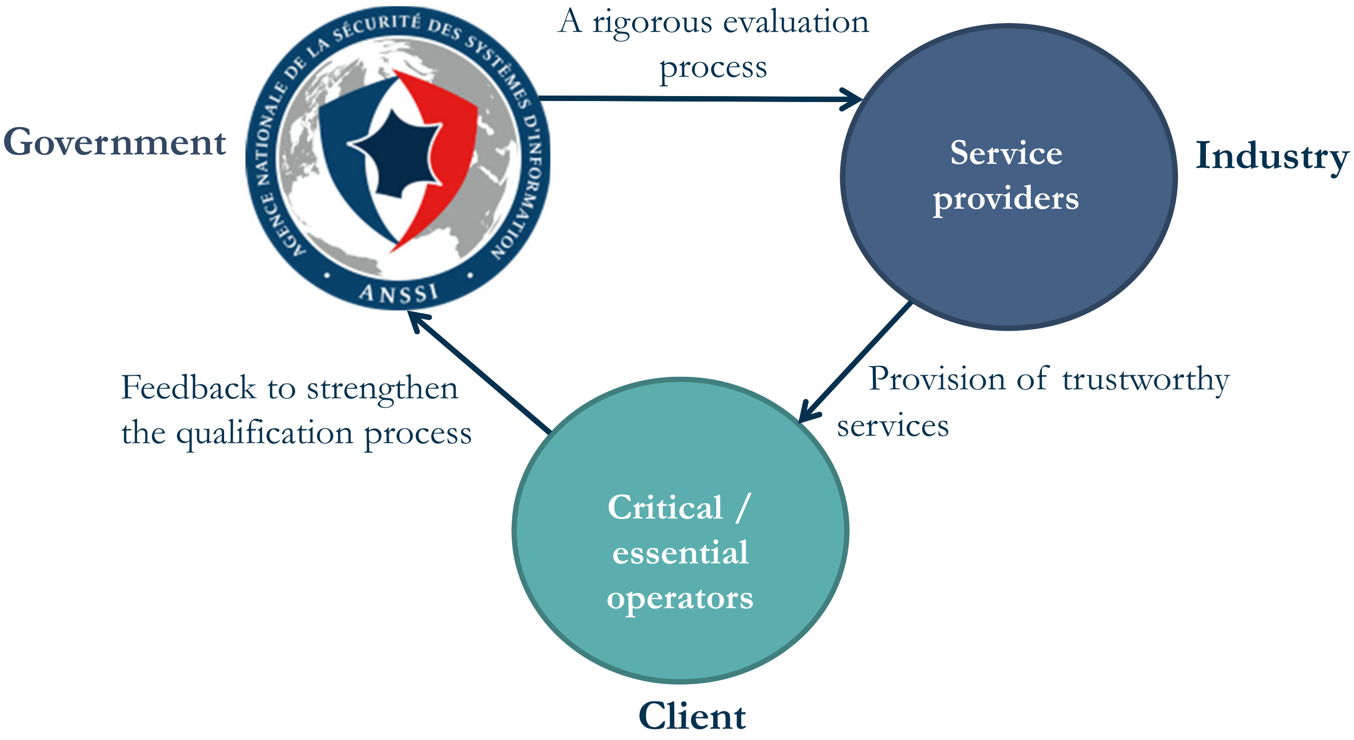
They must comply with strict requirements set in public reference documents:
(Requirements reference document for PASSI / PDIS / PRIS / Secnumcloud / PAMS)

These requirements cover following points:

- General requirements to be met by the service provider
- Activities description, tasks to be performed, skills needed
- Information protection
- Organization of the service provider and governance
- Quality and level of service

Trusted Service Providers

ANSSI has established a challenging and efficient process allowing the qualification of private “Trusted Service Providers”.



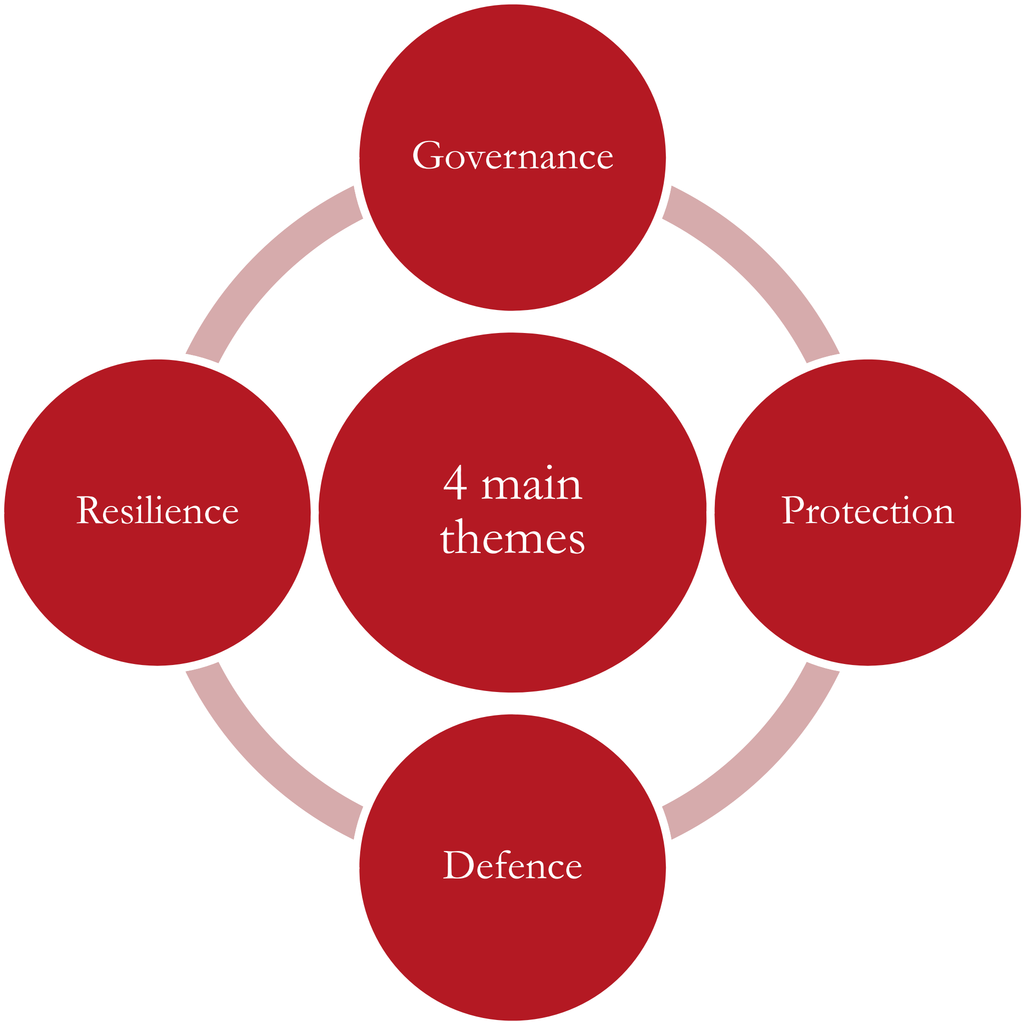
Government
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI
A rigorous evaluation process
Service providers
Industry
Provision of trustworthy services
Critical / essential operators
Client
Feedback to strengthen the qualification process

23 Security Rules (1/3)

Security measures:

- Organisational, risk management, technical
- In line with Cooperation Group's Reference document[1]

Scope : essential information systems (EIS), identified by OES based on an **impact analysis**



Notes : (1) https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

23 Security Rules (2/3)

Managing cybersecurity governance

❑ IT systems security policy:

- setting security goals and generic security measures for EIS
- scheduling training & awareness plans
- setting procedures for *homologation*, audits, incidents, crisis management

❑ Managing risks: risk analysis, audits conducted in a PASSI-compliant way, mandatory approval procedure for residual risks acceptance

❑ EIS mapping

Managing cybersecurity defence

❑ Comprehensive event logging + correlation & analysis in a PDIS-compliant way

❑ Detection systems operated in a PDIS-compliant way

❑ Security incidents handling in a PRIS-compliant way

Managing cybersecurity resilience

❑ ANSSI PoC appointment and elaboration of a crisis management procedure

23 Security Rules (3/3)

Managing cybersecurity protection

□ Identity and access management measures:
- use individual accounts
- change IT resources authentication secrets, use strong passwords
- manage and review acces rights

□ Use dedicated administration accounts and systems

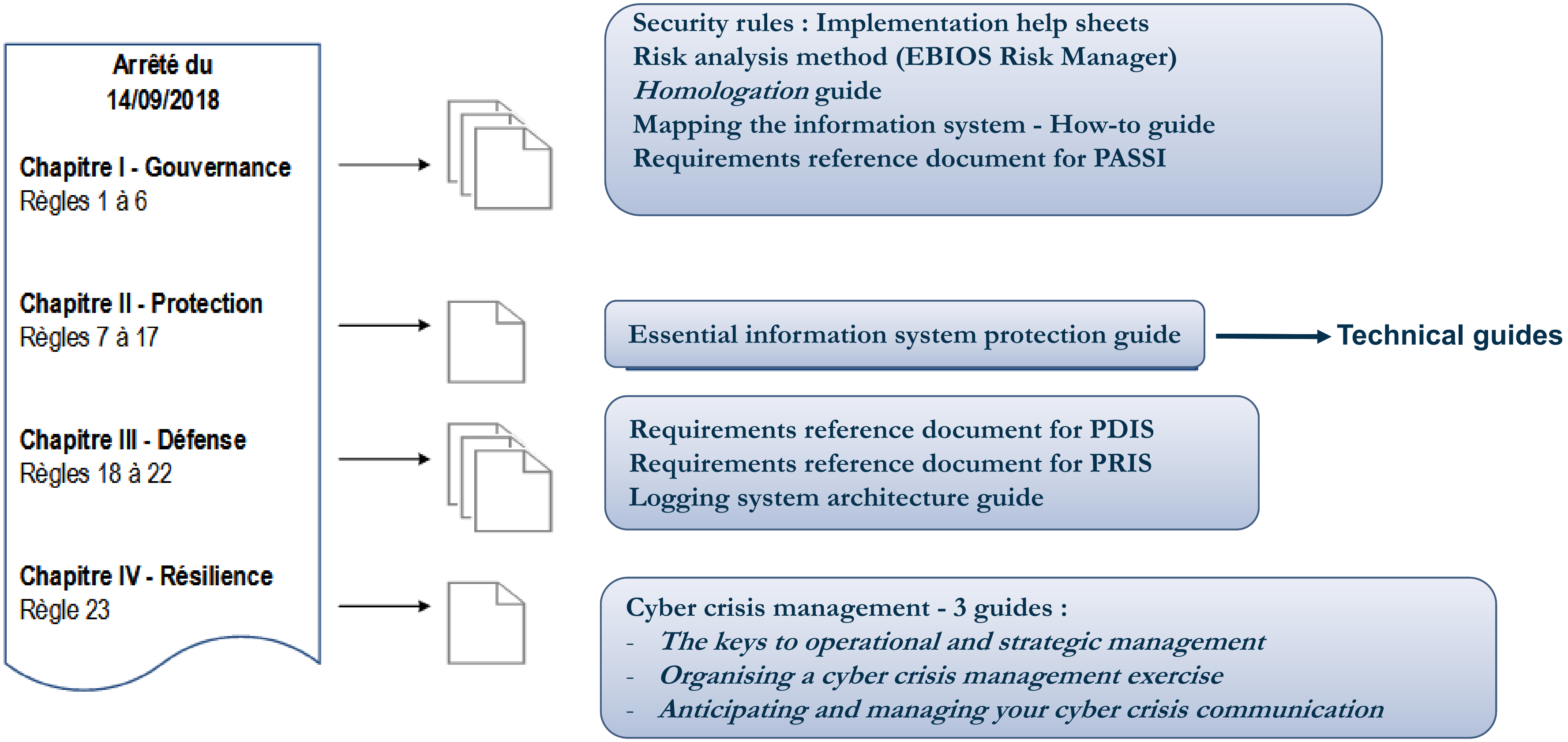
□ In-depth defence :
- segregate systems, filtering rules on system's limits and between sub-systems
- remote connections : dedicated controlled terminals, authentication and encryption mechanisms
- harden systems : uninstall unnecessary apps, control removable devices

□ Ensure security maintenance of EIS :
- elaborate a security maintenance procedure
- watch cyber alerts and security updates from CERTs and providers
- implement a patch management process (patch integrity check and impact assessment, etc.)
- implement specific security measures (e.g. segregation) for outdated systems

□ Regularly evaluate indicators on threat exposure

□ Physical and environmental security

Many guides to understand How to implement the security rules



Arrêté du 14/09/2018

Chapitre I - Gouvernance
Règles 1 à 6

Chapitre II - Protection
Règles 7 à 17

Chapitre III - Défense
Règles 18 à 22

Chapitre IV - Résilience
Règle 23

Security rules : Implementation help sheets
Risk analysis method (EBIOS Risk Manager)
Homologation guide
Mapping the information system - How-to guide
Requirements reference document for PASSI

Essential information system protection guide → **Technical guides**

Requirements reference document for PDIS
Requirements reference document for PRIS
Logging system architecture guide

Cyber crisis management - 3 guides :

- *The keys to operational and strategic management*
- *Organising a cyber crisis management exercise*
- *Anticipating and managing your cyber crisis communication*

Maritime and NIS directive : Who is concerned ?

NIS directive V1 :

- The most important French maritime ports
- Some river ports and inland companies
- Some shipping companies

NIS directive V2 : wider scope imposed by the directive

- Article 2 – scope :

  This Directive applies to public and private essential and important entities of a type referred to in Annex I and Annex II that provide their services or carry out their activities within the Union and which meet or exceed the threshold(*) for medium-sized enterprises within the meaning of Commission Recommendation 2003/361/EC

- Annex I – Sectors of high criticality

(*) employs more than 50 persons or annual turnover and/or annual balance sheet total more than EUR 10 million

Maritime and NIS directive : Who is concerned ?

Sector	Subsector	Type of entity
Transport	Water	Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004, **not including the individual vessels operated by those companies**
		Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC, including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC

www.ssi.gouv.fr

Thank you for your attention