French view on the NIS Diretcive transposition

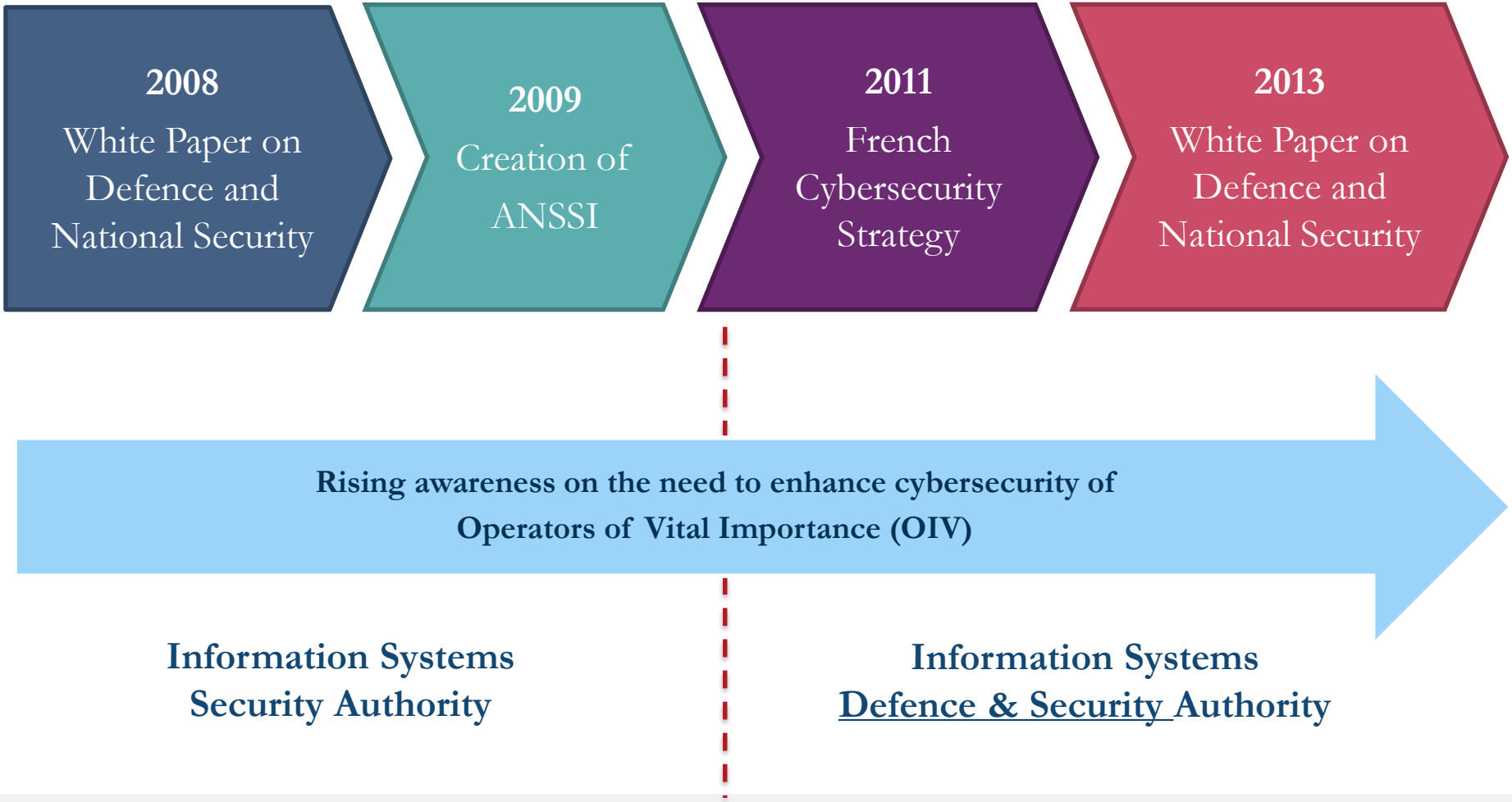
Cybersecurity Framework in France - ANSSI

> 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 responsability**, which reports to the General Secretary for Defence and National Security.

> ANSSI has 2 mains missions: **prevent** and **react** to cyber attacks.

Cybersecurity Framework in France - From government to critical infrastructures



CIIP - An existing critical infrastructures protection framework

More than 200 critical infrastructure operators ("Operators of Vital Importance") identified, since 2006.


Food


Telecom & broadcasting


Civilian administration


Energy


Health


Space & Research


Military activities

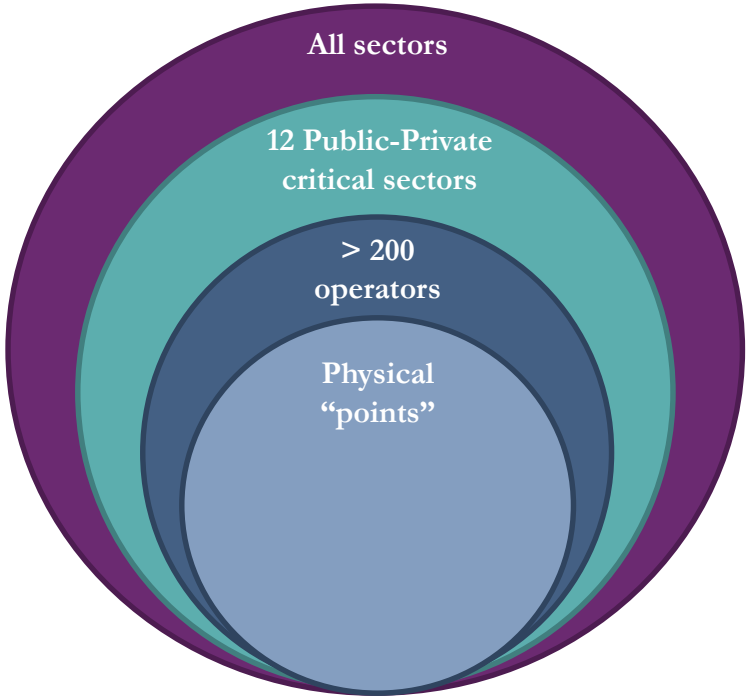

Transport


Water


Industry


Justice

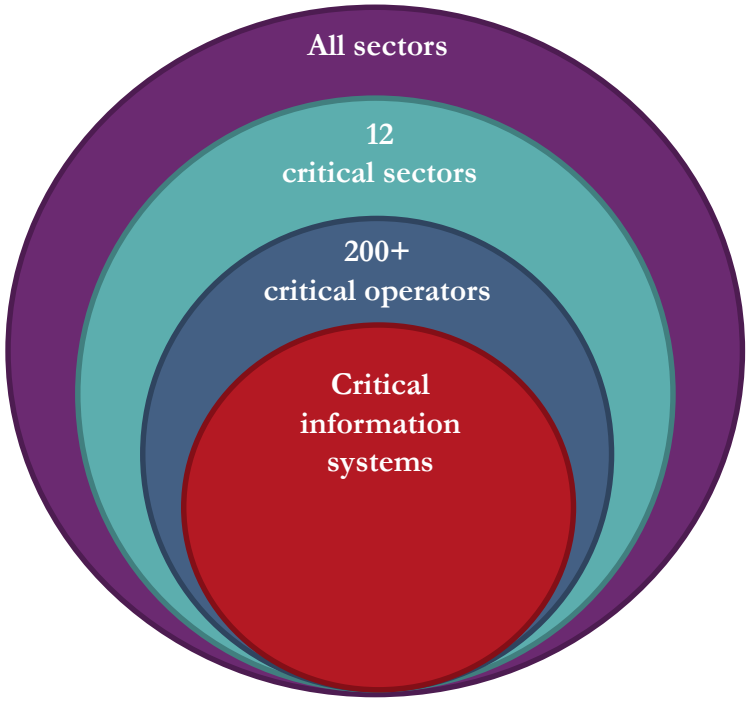

Finance



The CIIP law

Adopted in December 2013, the law aims at reinforcing the cybersecurity of critical operators and allows ANSSI – and other State bodies – to further support them in the event of a cyberattack against their critical information systems.

- The new framework will apply to all public and private critical operators already designated.
- In addition to their physical points, operators will need to identify their "critical information systems".
- Dedicated security measures will complement existing cybersecurity objectives.



The CIIP law

The law provides with 4 set of measures

SECURITY REQUIREMENTS ANSSI will impose to the operators a set of technical and organisational rules	**INCIDENTS NOTIFICATION** ANSSI shall be notified directly by operators of incidents occuring on their critical information systems.
INSPECTION ANSSI can trigger security audits led by itself, another State authority or a Trust service provider.	**MAJOR CRISIS** ANSSI can impose cybersecurity measures in case of major crisis, declared by the Prime Minister.

NIS - Strategic objectives

- A dynamic interministerial process to identify a new set of operators that are essential to economic and societal activities : the operators of essential services

- ANSSI will impose to these operators a set of technical and organizational rules very similar to the rules applying to the critical operators

Calendar and first challenges for the transposition

- Constrains : French presidential election in May and June 2017
- Promulgation of the law expected in beginning 2018
- Regulation : Decree to establish the list of essential services and application measure for each operators
- Execution act for the rules regarding he functionment of the cooperation group published in February 2017
- Bill submitted to ministries in May

Calendar for the transposition

Where do we stand today

Interministerial meeting of 09/10/2017 outcomes:

- A dedicated law to transpose chapters IV and V
- ANSSI designated as single competent autority for the cooperation group;
- CERT-FR designated as single French CSIRT for the CSIRT Network ;
- Prime minsister will establish the list of essential services and the list of OES on the proposition of ministries or ANSSI;
- Prime minister will define security rules for OES information systems

Challenge N°1 - Identification of the OES

- In the critical sectors already defined, the operators of essential services will be of the same nature as the critical operators (airports, hospitals, electricity suppliers…) but less sensitive.

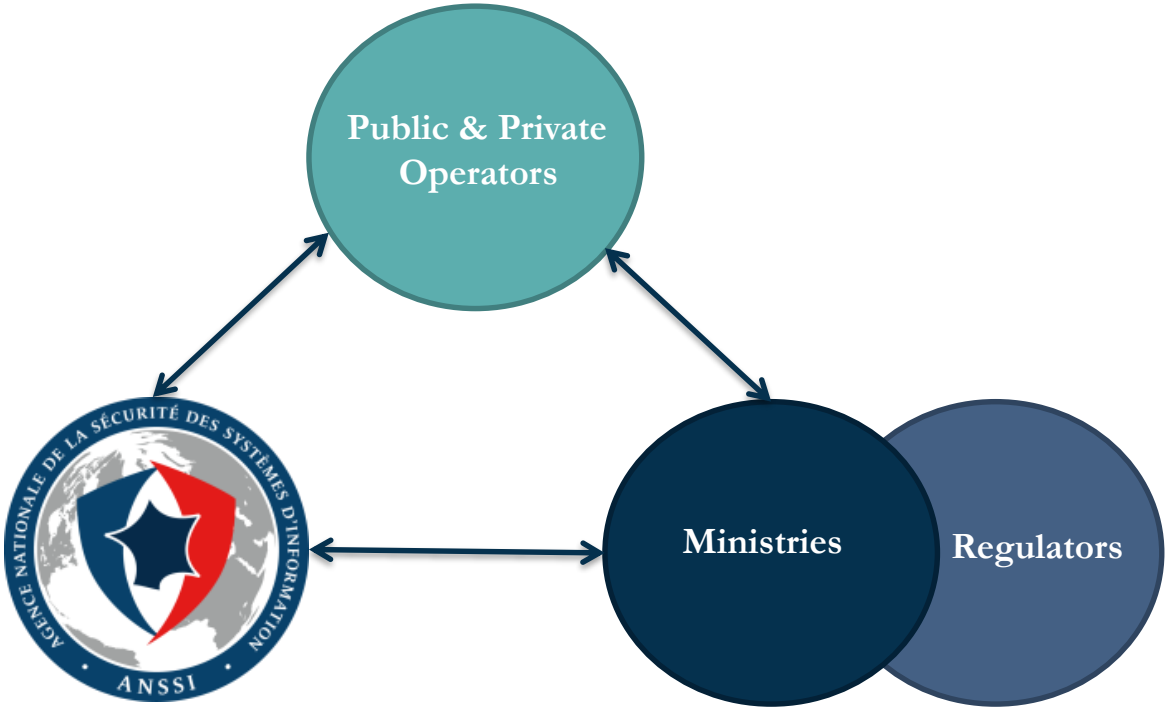
  The NIS directive covers many more companies. Are concerned and considered as OES :
  - Industrial production sites
  - Telecommunications operators
  - Transport companies
  - Hospitals, etc.

- Operators of essential services might be identified in other areas of activity (democratic life, cybersecurity industry, tourism…)

- Methodology: Mix of quantitative and qualitative criteria

Challenge N°2 – Working with the Private sector (RETEX)

Starting in late November 2014, working groups led by ANSSI were set up to define with the operators how core provisions would concretely apply.



Challenge N°3 – Articulation with CIIP framework

Art 22 LPM (Code of Defense)

OIV

→ National Security

→ Classified information

Dedicated law

OES

→ Internal maket

Stakeholders essential to the functioning of the economy and society

Challenges

- Apply the same rules to non OIV actors essential to the functioning of the economy and society
- Harmonize the different frameworks of EU member states
- Avoid new requirements for IS already submitted to the LPM

Challenge N°4 – Reach an acceptable security level

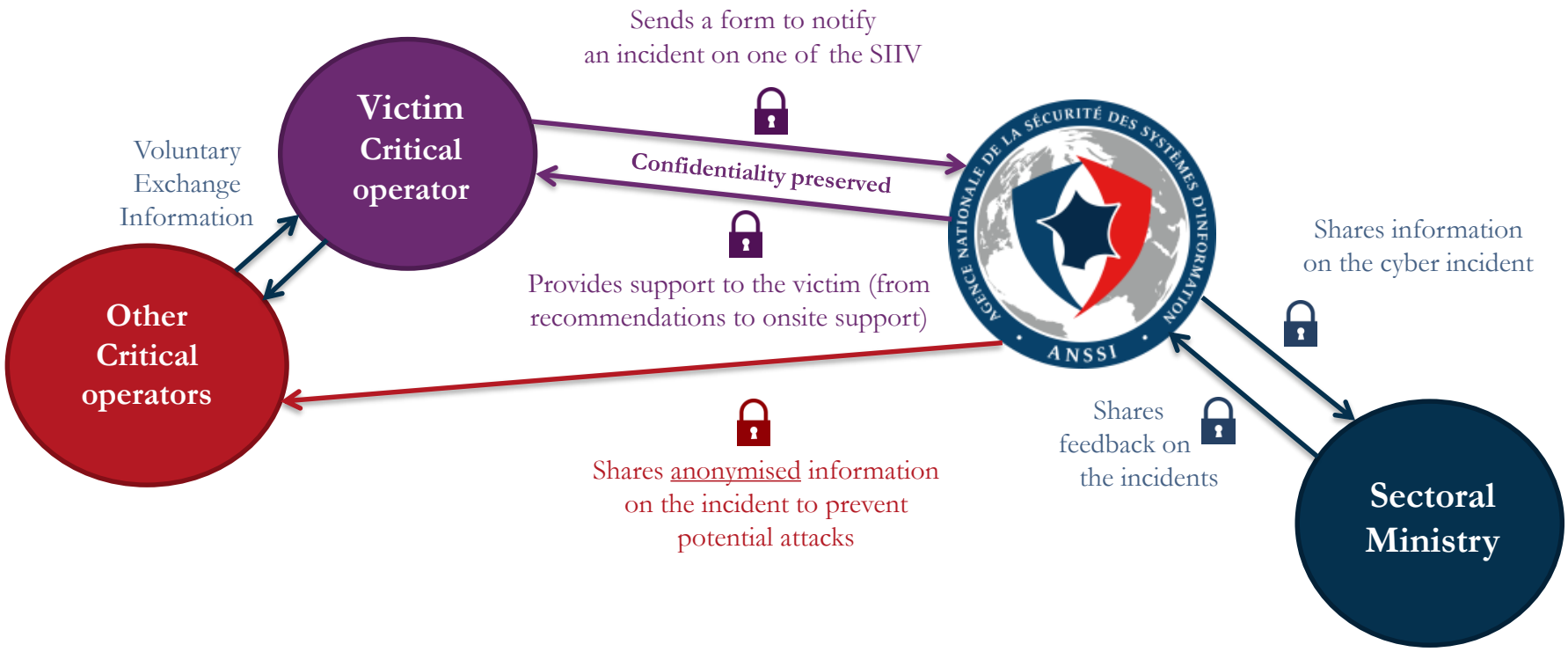
20 categories of security rules were elaborated and agreed upon by all operators : they are preventive actions aiming at reducing the risks of success for most cyberattacks.

Key characteristics

- Tailored cybersecurity measures.
- Mostly basic cybersecurity measures.
- Taking into account ANSSI's and the operators' operational experience and existing international standards.
- **95 % common** to all the sectors. But, depending on the sector's maturity, the timelines for application can differ (delays not public).
- Apply only to the operators' critical information systems.

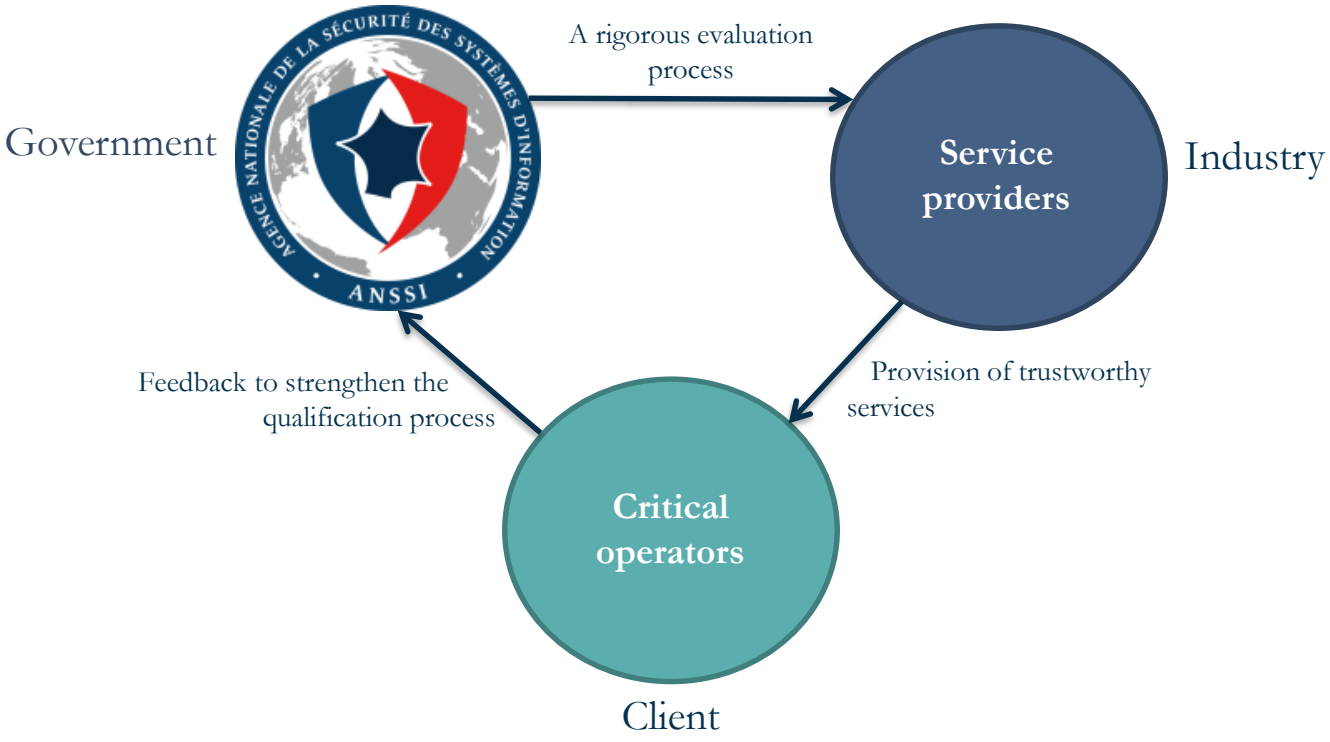
Note: the law will includes sanctions in case operators would not respect their obligations.

Challenge N°5 – Efficient Incident notification



Challenge N°6 – Assistance to the OES

In order to facilitate the implementation of the CIIP law, ANSSI has established a challenging and efficient process allowing the qualification of private "Trust Service Providers".



General overview- Adapt the security level to the risk