LOI DE PROGRAMMATION MILITAIRE

INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

Paralyser un Etat avec des cyberattaques, c'est possible

- Coupure internet pour toute l'Arménie et une partie de la Géorgie

Cause =

Section d'une fibre en entrée du pays

- 23 Décembre 2015 – Ukraine = 230k foyers privés d'électricité pendant près de 6h

Cause =

Cyber-attaque sur la compagnie ukrainienne Prykarpattyaoblenergo

Cyber-attaque en Ukraine

- Printemps 2015 : campagne de spear-phishing auprès de l'IT des compagnies d'électricité
- Eté – Automne : Intrusion et développement des malwares/firmwares. Mise en place de la stratégie.
- 23 Décembre : Déclenchement du malware

Extinction des centrales électriques

- Utilisation d'une session d'un opérateur
- Extinction à distance de 30 transformateurs électriques
- Installation d'un firmware modifié sur des « serial-to-ethernet » en empêchant le fonctionnement des commandes à distance

Qu'est-ce que la loi de programmation militaire ?

LOI DE PROGRAMMATION MILITAIRE 2014-2019

Les objectifs de la politique de défense et de la sécurité nationale

NEW

- Cyberattaques
- Systèmes d'Information d'Importance Vitale
- Sécurité informatique

ANSSI

- Etablissement de règles de sécurité nécessaires à la protection des Systèmes d'Information d'Importance Vitale (SIIV)
- Obligation d'informer l'Etat pour tout incident sur les SI des OIV

OPÉRATEUR D'IMPORTANCE VITALE

- Secteurs d'Activités d'Importance Vitale

- Activités civiles de l'Etat
- Activités militaires de l'Etat
- Activités judiciaires
- Espace et recherche
- Industrie
- Energie
- Transports
- Fiances
- Communication, audiovisuel et information
- Gestion de l'eau
- Santé
- Alimentation

~218 OIV

ÉTABLISSEMENT	INSTALLATIONS	OUVRAGES

Dont la destruction ou l'avarie peut présenter un danger grave pour la population

LPM ET SES IMPACTS

- Compréhension de la LPM

LÉGAUX

- ☐ Adapter la LPM aux contraintes juridiques de l'OIV
- ☐ Des OIV peuvent avoir des SIIV à l'international
- ☐ Appliquer la LPM en fonction de la CNIL et des lois déjà en place pour les SAIV

ORGANISATIONNELS

- ☐ Gouvernance
- ☐ Gestion de cyber-crise
- ☐ Veille stratégique et technologique
- ☐ Sensibilisation des utilisateurs

TECHNOLOGIQUES

- ☐ Analyse de l'existant
- ☐ Maîtrise des risques
- ☐ Système de détection d'incidents
- ☐ Reporting à l'ANSSI

FINANCIERS

- ☐ Coût mise en place LPM
- ☐ Coût audit annuel
- ☐ Provisions
- ☐ Budget MCO cybersécurité

MISE EN CONFORMITÉ DE LA LPM

1. Cadrage
2. Identifier SIIV et cartographier les SIIV
3. Mise en place des règles de sécurité
4. Détection incidents et lien avec l'ANSSI
5. Gestion des incidents
6. Audit

1. LE CADRAGE

Corrélation du risque cyber-sécurité et de expertise de l'attaquant		Risque cyber-sécurité		
		Sécurité à l'état de l'art (sécurité prédictive et proactive)	Sécurité périmétrique classique (physique, logique)	Pas de sécurité
Expertise	Cyber-mafia / Gouvernement (cyber-terrorisme)			
	Hacker expert (hacker isolé, virus, ...)			
	Débutant (Utilisateur)			

Risque faible Risque moyen Risque élevé

CADRAGE

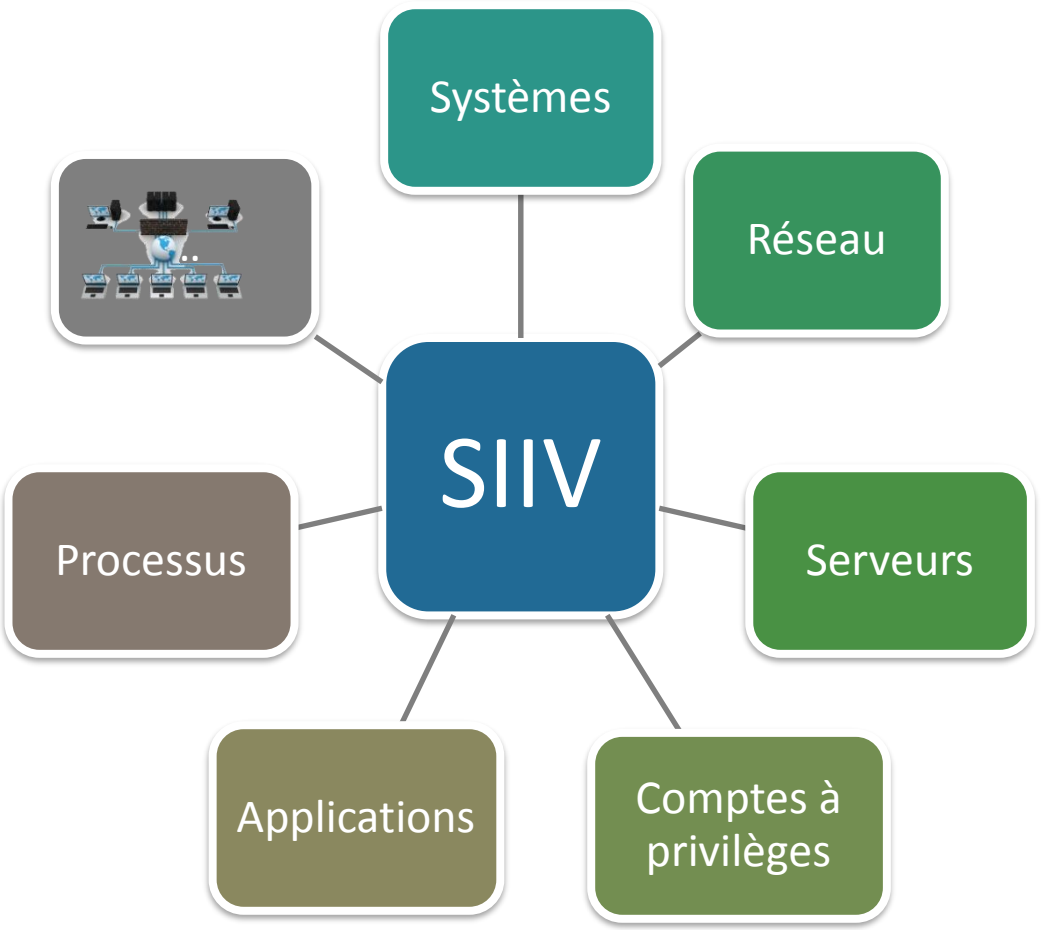
- Analyse de risques
- Aide à la compréhension des enjeux de la LPM et préparation à sa mise en place
- Explicitation du décret sectoriel et guide d'application des règles pour le client

OBJECTIFS

- PSSI
- Plan de Sécurité Opérateur

2. IDENTIFICATION SIIV ET CARTOGRAPHIE SI

- Comment appliquer la LPM dans une entreprise ?



IDENTIFICATION

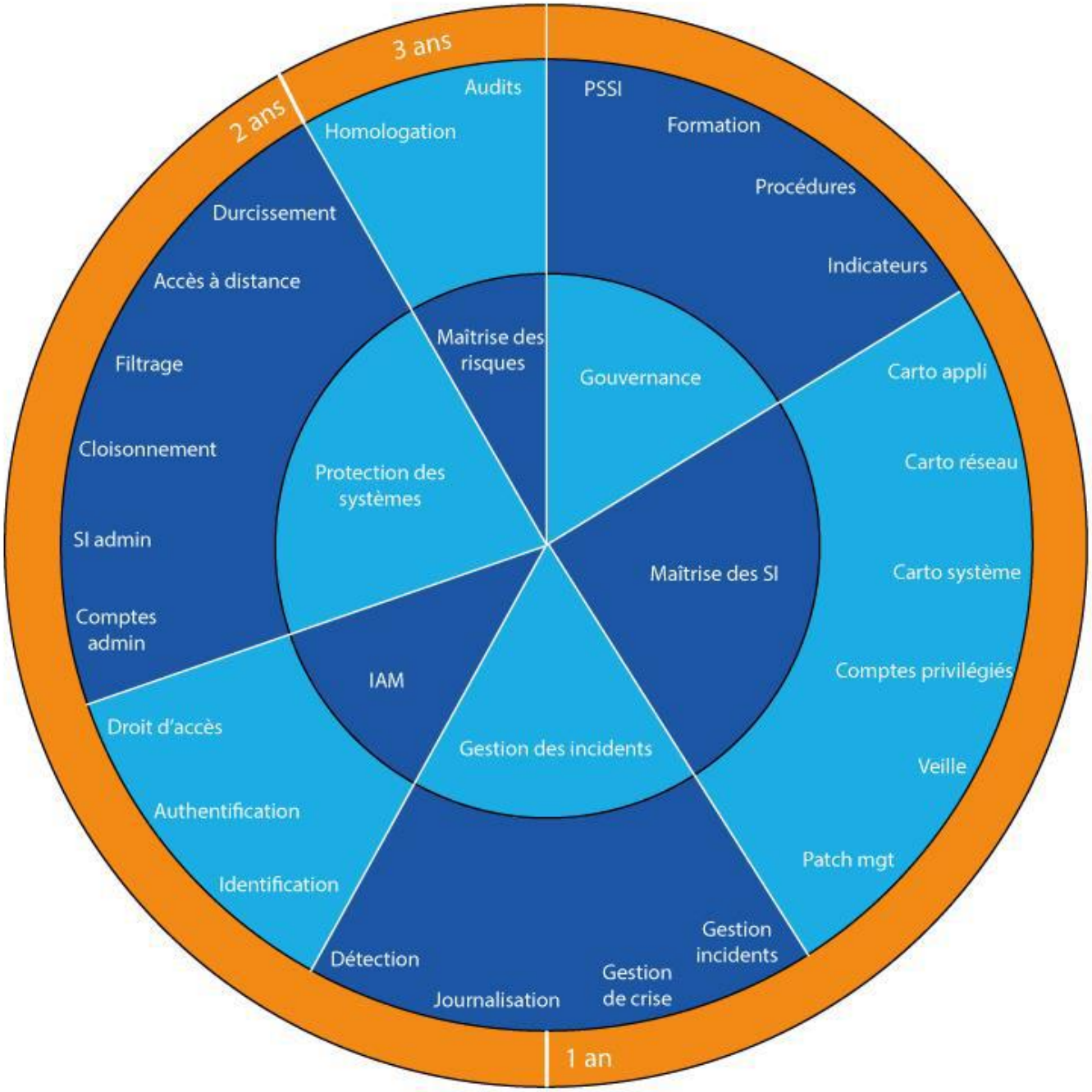
- Déterminer quels sont ses SI d'Importance Vitale
- Réaliser une cartographie complète et détaillée des SIIV

OBJECTIFS

- Plan de Sécurité Opérateur

MESURES DEMANDEES

- Comment appliquer la LPM dans une entreprise ?



DÉTECTION D'INCIDENTS

- Comment appliquer la LPM dans une entreprise ?

JOURNALISATION

- SIEM
- SI dédié avec 6 mois de conservation minimum

DETECTION D'INCIDENTS

- Sonde d'analyse de fichiers et de protocoles
- Certifié par l'ANSSI

POINT DE CONTACT

- Déterminer un contact 24/7 avec l'ANSSI

GESTION D'INCIDENT

- Comment appliquer la LPM dans une entreprise ?

PROCÉDURE DE GESTION DE CRISE EN CAS D'ATTAQUES INFORMATIQUES MAJEURES

- Plan de Continuité d'Activité
- Plan de Reprise d'Activité
- Gestion des incidents avec l'ANSSI

Audit

AUDIT ANNUEL PAR UN PASSI

- Homologation de sécurité du SI et conformité LPM

- Objectif de conseil auprès du client OIV
- Processus d'audit défini par l'ANSSI
- Auditeurs qualifiés PASSI

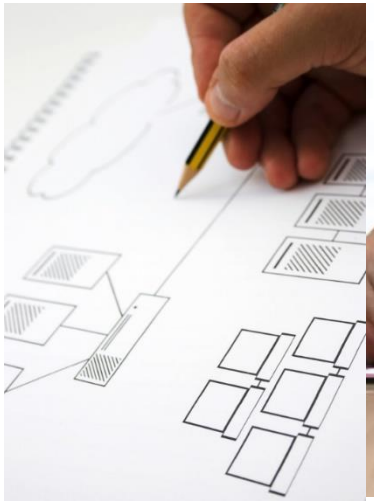
- Audit architecture
- Audit de configuration
- Tests d'intrusion
- Audit organisationnel et physique
- Audit de code source

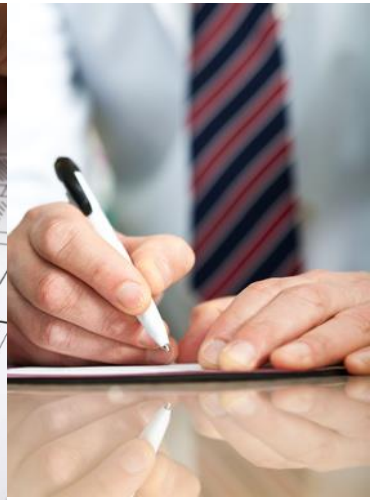
PASSI

- Qualification

PRESTATAIRE D'AUDIT DE SECURITE DES SYSTEMES D'INFORMATION

- Permet d'auditer les OIV
- Permet d'être reconnu comme prestataire de qualité auprès des entreprises





PREPARATION PASSI

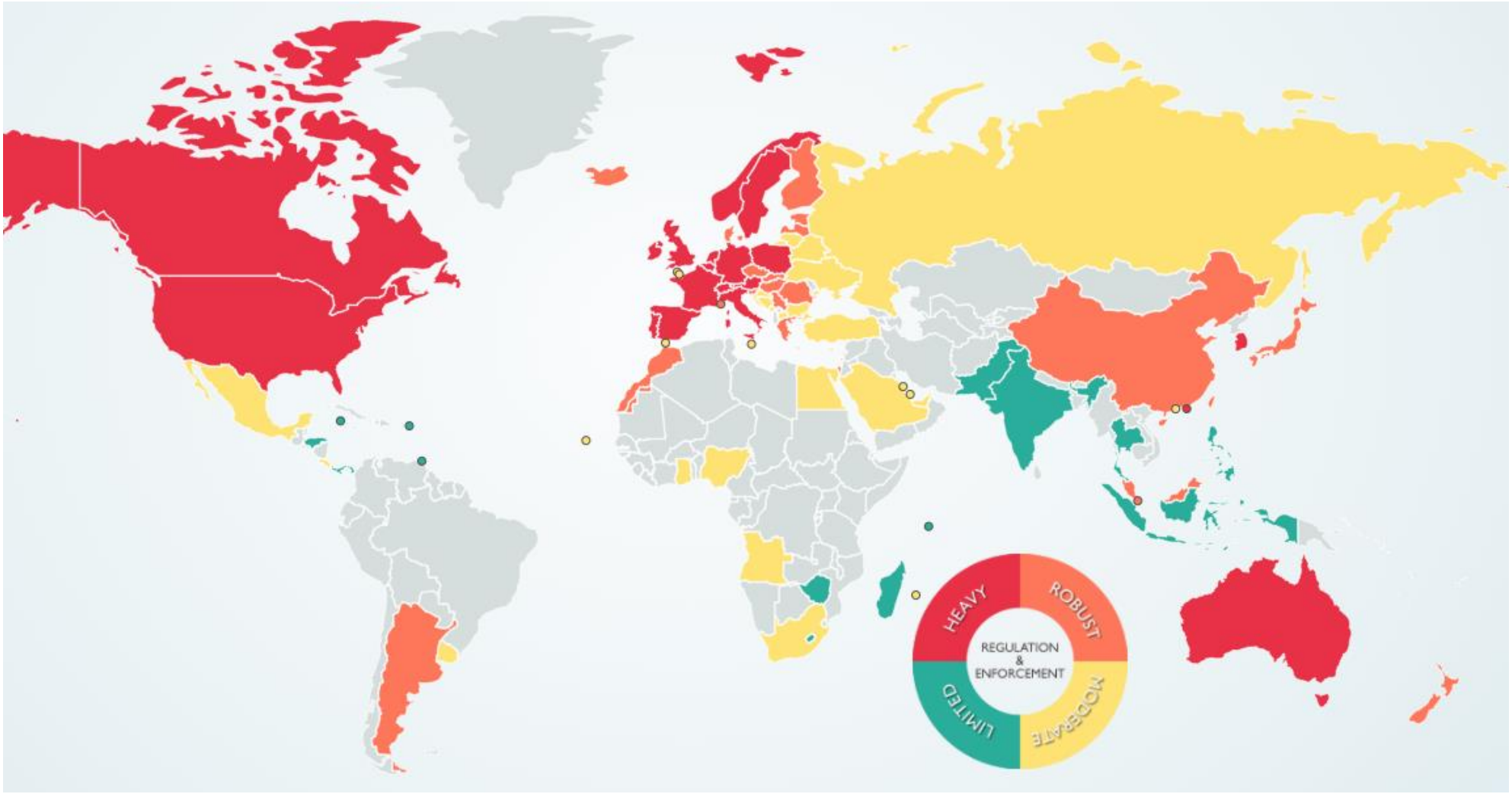
SI Diffusion Restreinte	Audit	Auditeurs
▪ Mise en place de ce SI dans le Cloud ▪ Informations confidentielles Diffusion Restreinte ▪ Analyse de risques SI DR	▪ Processus d'audit ▪ Documents type	▪ Sensibilisation : LPM, PASSI, RGSv2, ISO 19011, …

A BIT MORE OF GDPR

GENERAL DATA PROTECTION REGULATION

INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

Data protection laws around the world

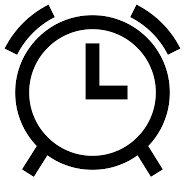


Source: www.dlapiperdataprotection.com

General introduction

A new European regulation

A single text with limited member states deviations



Date of entry into force: 25 may 2018

Extraterritorial scope (not just the EU)

The **G**eneral **D**ata **P**rotection **R**egulation will, among other things**:**

- ✓ widen the definition of personal data
- ✓ tighten the rules for obtaining valid consent to use personal information
- ✓ introduce a common data breach notification requirement (72h)
- ✓ failure to comply could lead to a fine of up to the greater of EUR20m or 4% of annual worldwide turnover
- ✓ require privacy by design & by default
- ✓ Introduce the concept of one-stop shop for personal data inquiries

GDPR: focus on territorial scope

The GDPR applies in the following cases:

1

Processing of personal data in the European Union (regardless of whether the processing takes place in the Union or not)

2

Processing of personal data of data subjects who are in the UE by a controller or processor not established in the Union.

The processing must be related to:

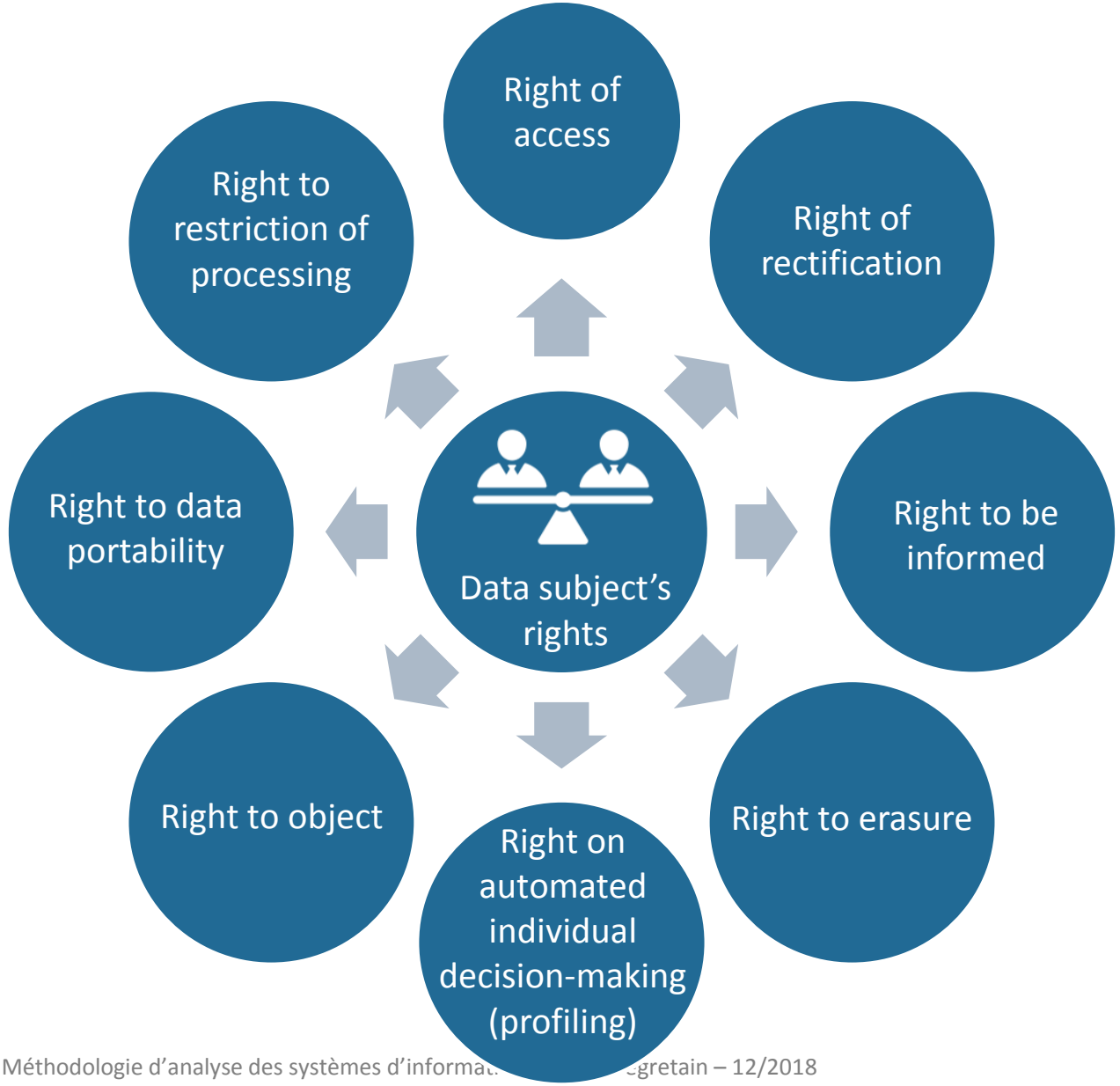
- The offering of goods or services to data subjects in the UE
- The monitoring of their behavior (when it takes place within the UE)

What personal data do I have the right to process?

- Personal data categories are generally as follows:

Personal data types	Personal data categories
Common personal data	Civil status, identity, identification data
	Personal life (living habits, marital status, etc. –excluding sensitive or dangerous data)
	Professional life (résumé, education and professional training, awards, etc.)
	Economic and financial information (income, financial situation, tax situation, etc.)
	Connection data (IP addresses, event logs, etc.)
	Location data (travels, GPS data, GSM data, etc.)
Personal data perceived as sensitive	Social security number
	Biometric data
	Bank data
Sensitive personal data in the meaning of [DP-Act][1]	Philosophical, political, religious and trade-union views, sex life, health data, racial or ethnic origin, data concerning health or sex life
	Offenses, convictions, security measures

Focus on the data subject's rights



Conditions of processing

Personal data in personal data processing must be:

Fairly and **lawfully** processed

Consent must be obtained before any processing or depend on a contractual relationship or a legal obligation of the data controller

Processed for limited purposes

The purpose must be determined upstream and the processing must correspond to the purpose determined

Adequate, relevant and not excessive

With regard to the purposes, only the relevant data must be processed

Accurate and where necessary up-to-date

Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay

Not be kept for longer than is necessary

The retention of personal data must be limited in time in relation to the defined purposes

Processed in line with the data subjects rights

The data subjects rights must be respected

Not transferred to other countries without adequate protection

Data transfers must be limited to EEA countries and countries that provide security guarantees. These countries are listed by the supervisory authorities. Others methods nevertheless allow data transfers to be made in other countries (Privacy Shield, etc)

Privacy Impact Assessment

- PIA is a risk assessment with focus on PII
- Purpose to build and demonstrate the implementation of privacy protection principles so that data subjects retain control over their personal data.
- CNIL methodology is based on EBIOS

- https://www.cnil.fr/en/PIA-privacy-impact-assessment-en

Privacy Impact Assessment by CNIL

- Build the system that ensures compliance with privacy protection principles
- Gain a good understanding of the causes and consequences of risks (included potential privacy breaches)

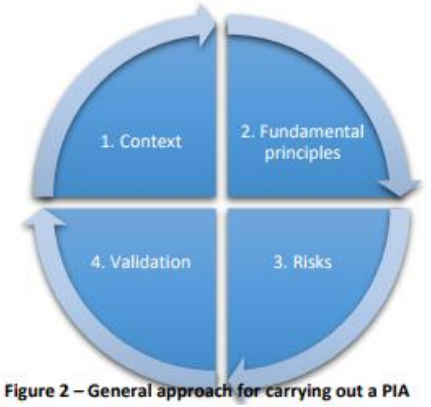


Figure 2 – General approach for carrying out a PIA

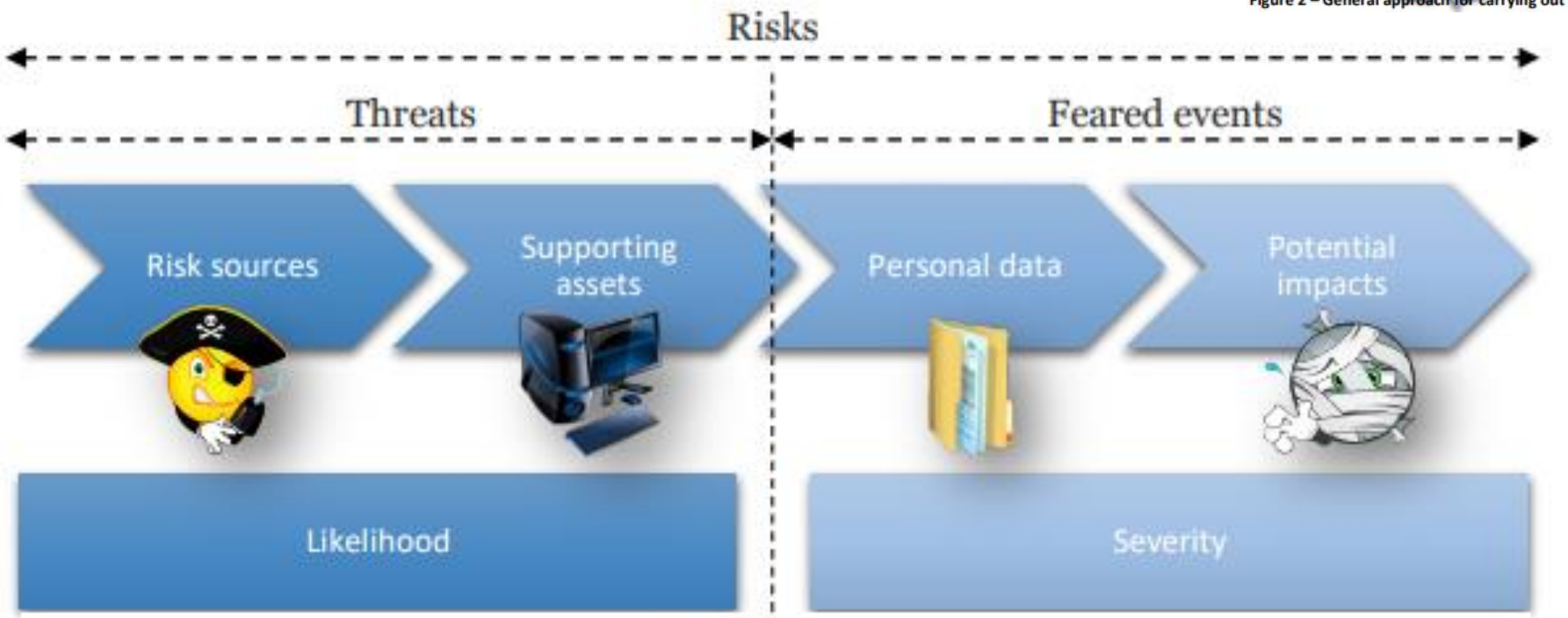


Figure 3 – Risk components

Security

- The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing.
- However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:
  - the pseudonymisation and encryption of personal data;
  - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
  - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

FIN DU COURS POUR MOI

What society thinks I do

What my mom thinks I do

What my friends thinks I do

What my clients thinks I do

What I think I do

What I actually do