PRC Cyber Security Law (CSL) & Multi Level Protection Scheme 2.0 (MLPS 2.0)
27 juin 2019 - IHEDN – Paris

Isabelle Hajjar
Head of Compliance
Cybersecurity & Data Privacy
contact@tek-id.com

Marguerite Bilalian
Avocat à la Cour

mail@bilalian-avocats.com

02 La China Cybersecurity Law ('CSL') en quelques mots

- → **Entrée en vigueur le 1er juin 2017**;
- → Dans le contexte général du renforcement et de la **sophistication de l'arsenal législatif Chinois** ;
- → Et de la création de la Cyberspace Administration of China (CAC) en 2012 ;
- → Aux fins d'accroitre les pouvoirs de surveillance et conforter un contrôle total sur le cyber espace ;
- → Il s'agit d'une **loi 'parapluie' et 'fourre-tout'** posant un cadre général ;
- → La philosophie de la CSL s'inscrivant en droite ligne dans la Stratégie Nationale de Cybersécurité de la Chine, publiée en 2016, et affirmant qu'"***il n'y a pas de sécurité nationale sans cybersécurité***".

03 Les entités soumises à la CSL

La CSL et la législation associée s'appliquent aux **Network Operators** (opérateurs de réseau) et **Critical Information Infrastructure Operators** (opérateurs d'infrastructure d'information essentielle (CIIO)

Les Network Operators - « N.O.s » - (opérateurs de réseau):

Les entités ou personnes possédant ou gérant un réseau informatique en Chine, et les prestataires de services réseau.

Avoir un site Internet, ou 5 ordinateurs connectés, ou une adresse IP fixe suffit pour être un N.O.

03 Les entités soumises à la CSL

Les **Critical Information Infrastructure Operators** - « CIIOs » - (operateurs d'infrastructures essentielles) sont les entités exploitant et/ou gérant **des installations réseau et systèmes d'information :**

→ **qui s'ils subissaient des dommages, destruction, perte de fonction, fuites ou pertes données, en résulterait une grave menace pour la sécurité nationale, l'économie nationale, les moyens de subsistance des personnes et l'intérêt public**;

→ **dans les domaines suivants:**

(1) les agences et entités gouvernementales, entités dans les secteurs de l'énergie, des finances, des transports, de la conservation de l'eau, de la santé et de l'hygiène, de l'éducation, de l'assurance sociale, de la protection de l'environnement et des services publics ;

(2) les réseaux d'information, Internet, les services cloud, big data et autres services de réseau d'information à grande échelle à destination du public ;

(3) les entités de recherche et de fabrication dans les secteurs tels que la science et la technologie pour la défense nationale, les grands équipementiers, les industries chimique, alimentaire et pharmaceutique, la fabrication industrielle;

(4) les organes de presse; et

(5) **autres entités clés**.

03 Les entités soumises à la CSL

Les **Guidelines for Cybersecurity Examination de juin 2016** précisent en outre que les éléments suivants peuvent être identifiés comme des CII (infrastructures essentielles) si l'une des conditions suivantes est remplie :

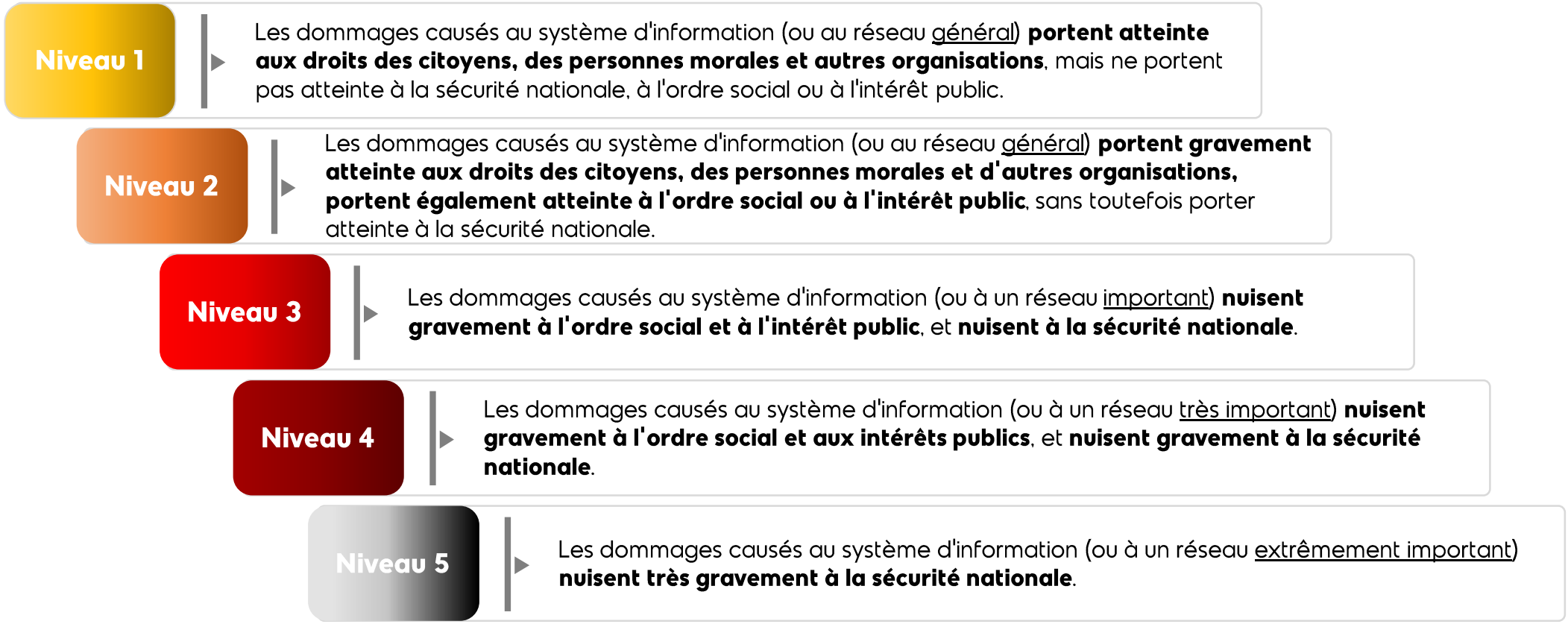
→ **Pour les sites internet** :
- Plus d'**1 million de trafic quotidien moyen** ;
- Si un incident de cybersécurité peut notamment entraîner la **violation des données personnelles de plus d'1 million de personnes** ;

→ **Pour les Plateformes** :
- **Plus de 10 millions d'utilisateurs** enregistrés, **ou plus d'1 million d'utilisateurs actifs par jour** ;
- Montant moyen des commandes ou du CA quotidien **> à 10 millions de RMB** ;
- Si un incident de cybersécurité peut notamment entraîner la **violation des données personnelles de plus d'1 million de personnes** ;

→ **Pour les infrastructures affectées à la production et aux opérations** :
- **Les Data Centers avec plus de 1500 racks standards** ;
- Si un incident de cybersécurité peut entraîner la **violation des données personnelles de plus d'1 million de personnes**.

04 Le périmètre de sino-sécurité : la CSL & le MLPS 2.0

Le Multi-Level Protection Scheme

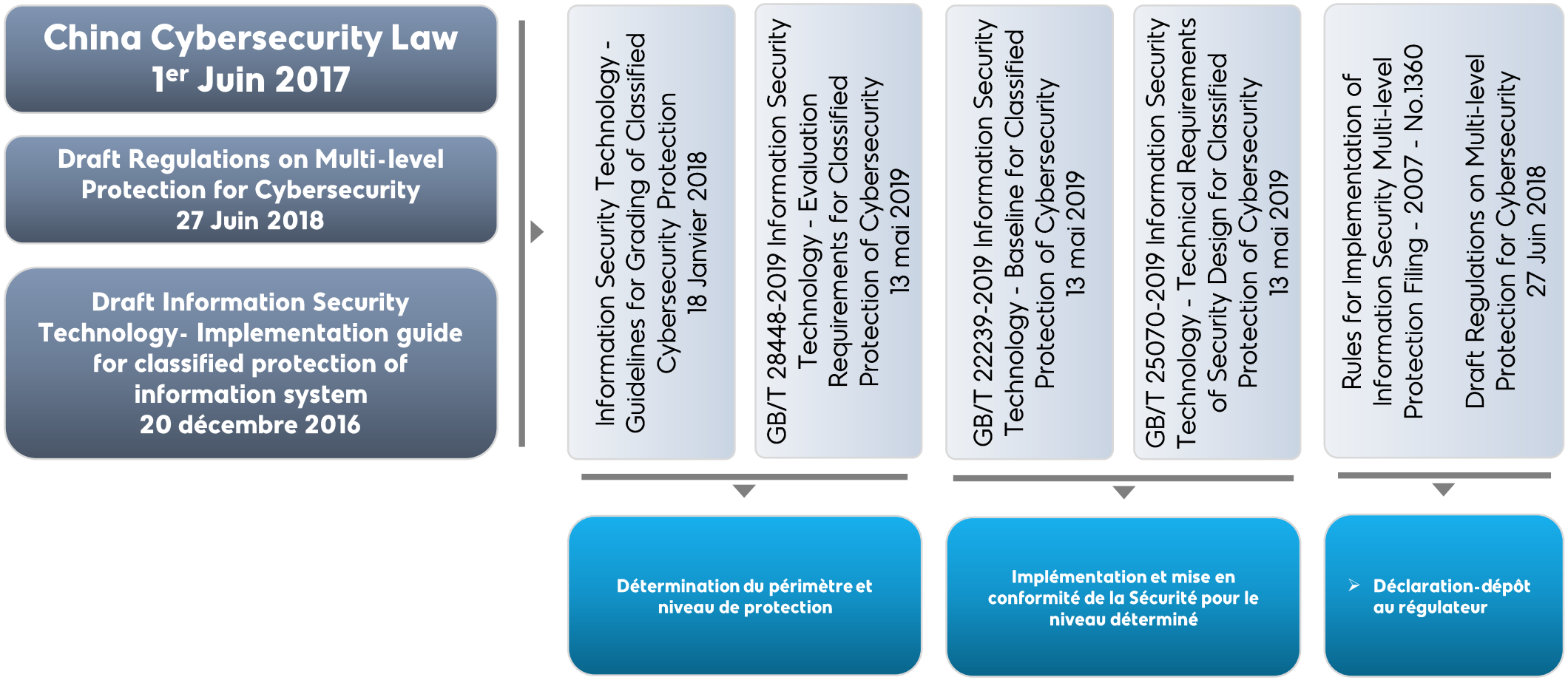


04 Le périmètre de sino-sécurité : la CSL & le MLPS 2.0

Comment déterminer son niveau MLPS ?

Conséquence d'un incident affectant les systèmes d'information, réseaux ou données	Importance du dommage		
	General	Important	grave
Atteinte aux droits des citoyens, des personnes morales et autres organisations	Niveau 1	Niveau 2	Niveau 3
Atteinte à l'ordre social ou à l'intérêt public	Niveau 2	Niveau 3	Niveau 4
Atteinte à la sécurité nationale	Niveau 3	Niveau 4	Niveau 5

04 Le périmètre de sino-sécurité : la CSL & le MLPS 2.0



04 Le périmètre de sino-sécurité : la CSL & le MLPS 2.0

Méthodologie de mise en conformité

Auto-détermination N.O / CIIO, du périmètre de la protection et du niveau de protection

- **Identification des domaines d'activité** ;
- **Identification, partition et description des SI** ;
- **Détermination du niveau de sécurité applicable** (MLPS) ;
- **Rapport de classification**.

Gap Analysis & plan de mise ne conformité

- **Analyse des écarts et lacunes** ;
- **Rapport d'analyse** ;
- **Elaboration et formalisation du plan de mise en conformité** ;
- **Implémentation du plan** ;
- **Réception** de l' implémentation **avec rapport de réception**.

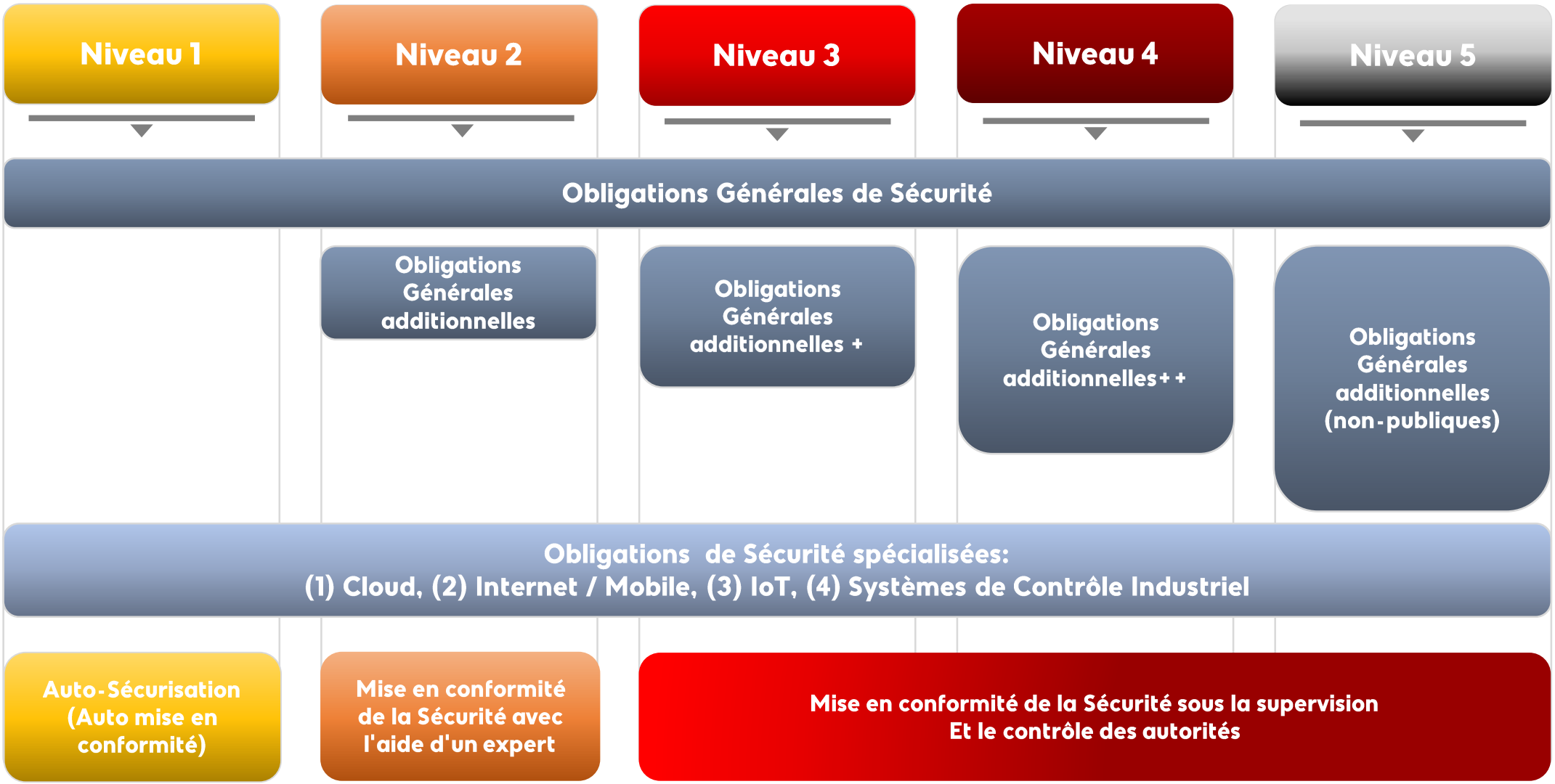
Dépôt de dossier, confirmation, approbation et certification

- **Evaluations par tierce 'expert' et rapport** ;
- **Préparation de la documentation de classification** ;
- **Dépôt de dossier auprès des autorités** ;
- **Tests / audits menés par les autorités** (niveau 3+) ;
- **Obtention de la confirmation / approbation / certification**.

Maintien en condition, management du changement et amélioration continue

- **Mise en place d'un monitoring** & **trainings réguliers** ;
- **Management du changement** ;
- **Plan de réponse, de gestion de crise et de continuité** ;
- **Documentation et notification des incidents** ;
- **Plan d'amélioration continue** ;

05 Les obligations de sécurité sous la CSL & le MLPS 2.0



05 Les obligations de sécurité sous la CSL & le MLPS 2.0

Niveau 1	Niveau 2	Niveau 3	Niveau 4

Obligations Générales de Sécurité - Obligations hautes sous la CSL

Network Operators (incluant CIIOs)

→ **Système et règles internes de gestion de la sécurité des SI et réseaux** ;

→ **Personnel dédié a la cybersécurité** ;

→ **Mesures techniques** contres les virus informatiques, attaques, etc. ;

→ **Conservation des logs pendant au moins 6 mois** ;

→ **Classification des données** ;

→ **Back-ups et encryption des données** ;

→ **Plans d'intervention d'urgence** ;

→ **Monitoring de la sécurité** et **audits et évaluations des risques** ;

→ **Coopération avec les autorités** ;

→ **Notification des incidents** aux autorités ;

→ **Identité réelle des utilisateurs clients** ;

→ **Contrôle du contenu** ;

→ **Sanctions pénales**.

05 Les obligations de sécurité sous la CSL & le MLPS 2.0

Niveau 1	Niveau 2	Niveau 3	Niveau 4

Obligations Générales de Sécurité - Obligations hautes sous la CSL

CIIOs

→ **Personnel dédié a la cybersécurité** (exigences +) ;

→ **Equipes de sécurité spécialisées** ;

→ **Training sécurité régulier de tous les employés** ;

→ **Plan de sauvegarde et de récupération** ;

→ **Tests réguliers du plan d'intervention d'urgence** ;

→ **Audits et évaluations de la sécurité et des risques annuels** ;

→ **Localisation** ;

→ **Sourcing et achat de produits certifiés**.

05 Les obligations de sécurité sous la CSL & le MLPS 2.0

Niveau 1	Niveau 2	Niveau 3	Niveau 4

Obligations Générales détaillées de Sécurité - référentiels / standards sous le MLPS 2.0

→ **Sécurité physique** des ressources IT ;

→ **Réseau de communication sécurisé** ;

→ **Limite de réseau sécurisée** ;

→ **Environnement informatique sécurisé** ;

→ **Système de gestion de la sécurité** ;

→ **Moyens / organisation de gestion de la sécurité** ;

→ **Management de la sécurité RH** ;

→ **Gestion de la construction de la sécurité** ;

→ **Maintien en condition de la sécurité et de la maintenance** ;

→ **Sourcing et achat de produits de sécurité**.

→ Mise en place d'un centre de gestion de la sécurité ;

→ Personnel spécialement affecté à la cybersécurité ;

→ Test réguliers, etc.

→ Personnel spécialement affecté à la cybersécurité : au moins 2 personnes, etc.

05 Les obligations de sécurité sous la CSL & le MLPS 2.0

Niveau 1	Niveau 2	Niveau 3	Niveau 4

Obligations spécialisées - Cloud - référentiels / standards sous le MLPS 2.0

→ **localisation de l'infrastructure** ;

→ **localisation des données personnelles et importantes** ;

→ **Gestion de la construction de la sécurité**.

→ Localisation des opérations de sécurité et de la maintenance

→ Centre de gestion de la sécurité

Obligations spécialisées - Internet / Mobile - référentiels / standards sous le MLPS 2.0

→ Environnement physique sécurisé ; **protection électromagnétique** ;

→ Limites sécurisées: **gateway approuvé** ;

→ **Applications mobiles approuvées et autorisées** ;

→ **Vérification des fournisseurs d'applications mobiles**, etc.).

→ Gestion des opérations de sécurité et de la maintenance,

05 Les obligations de sécurité sous la CSL & le MLPS 2.0

Niveau 1	Niveau 2	Niveau 3	Niveau 4

Obligations spécialisées -IoT - référentiels / standards sous le MLPS 2.0

→Environnement physique sécurisé : **choix de l'emplacement des senseurs** ;

→Limites sécurisées : **contrôle d'accès aux senseurs** ;

→Gestion des opérations de sécurité et de la maintenance : **contrôle physique régulier des senseurs**.

→Environnement informatique sécurisé+

Obligations spécialisées - Systèmes de contrôle industriel - référentiels / standards sous le MLPS 2.0

→Environnement physique sécurisé : **protection physique des équipements**, et maintenance ;

→Réseau de communication sécurisé : **ségrégation des systèmes de contrôle industriel**, etc.

→Gestion de la construction de sécurité : **sourcing et achat de systèmes de contrôle industriel sécurisés auprès de professionnels agrées**.

06 Du Cote de la France

- **Création de l'Agence Nationale de la Sécurité des Systèmes d'Information ('ANSSI') en 2009** ;
- Une première stratégie nationale de cybersécurité en 2011 ;
- **La loi de programmation militaire de 2013 comportant un volet cybersécurité concernant les Operateurs d'Importance Vitale ('OIV')** ;
- Une 2nde stratégie de cybersécurité en 2015, renforcée par la stratégie internationale de la France pour le numérique de décembre 2017 ;
- **La loi du 26 février 2018** de transposition de la directive européenne du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union - 'Directive NIS' - , **imposant des obligations de sécurité aux opérateurs de services essentiels (OSE) et aux fournisseurs de services numériques (FSN)** ;
- L'Appel de Paris du 12 novembre 2018 lors de la réunion à l'UNESCO du Forum de gouvernance de l'Internet, pour la confiance et la sécurité dans le cyberespace.

06 Les OIV sous la LPM

L'article 22 de la loi de programmation militaire de 2013 impose **aux Operateurs d'Importance Vitale (OIV)** le **renforcement de la sécurité de leurs systèmes d'information d'importance vitale (SIIV)**.

Les Operateurs d'Importance Vitale - « OIV » :

→ « Les opérateurs exploitant des établissements ou utilisant des installations et ouvrages, **dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation** ;

→ **dans les 12 secteurs suivants, identifiés comme stratégiques** :

- Activité Humaine :
  - ✓ Alimentation
  - ✓ Gestion de l'eau
  - ✓ Santé
- Activité régalienne :
  - ✓ Activités civiles de l'Etat
  - ✓ Activités judiciaires
  - ✓ Activités militaires de l'Etat
- Activité économique :
  - ✓ Energie
  - ✓ Finances
  - ✓ Transports
- Activité technologique :
  - ✓ Communications électroniques, audiovisuel et information
  - ✓ Industrie
  - ✓ Espace et recherche

06 Les OSE et les FSN sous la loi de transposition de la Directive NIS

Le décret d'application n° 2018-384 du 23 mai 2018 de la loi française de transposition de la Directive NIS vient également imposer **aux Operateurs de Services Essentiels (OSE) et aux Fournisseurs de Services Numériques (FSN) des obligations de sécurité leurs systèmes d'information**.

Les Operateurs de Services Essentiels - « OSE » :

→ Les entités **fournissant au moins un service identifié comme essentiel dans un secteur stratégique**, lorsque la fourniture de ce service est **tributaire des réseaux et systèmes d'information et qu'un incident les affectant aurait, sur la fourniture de ce service, des conséquences graves**, au regard de certains critères listés ;

→ **Des services essentiels identifiés dans les 15 secteurs considérés comme stratégiques** :

- ✓ Energie
- ✓ Transport
- ✓ logistique
- ✓ Banques
- ✓ Infrastructures de marchés financiers
- ✓ services financiers
- ✓ assurance
- ✓ social
- ✓ emploi et formation professionnelle
- ✓ éducation
- ✓ Santé
- ✓ fourniture et distribution d'eau potable
- ✓ traitements des eaux non potables
- ✓ infrastructures numériques
- ✓ restauration

06 Les OSE et les FSN sous la loi de transposition de la Directive NIS

→ **Les Fournisseurs de Services Numériques** - « FSN » :

(1) les place de marche en ligne (plateformes e-commerce),
(2) les moteurs de recherche en ligne, et
(3) les entités offrant des services cloud,

→ de plus de 50 salaries et ayant un chiffres d'affaires de plus de 10 millions d'Euros.

07 Du cote de la France - les obligations de sécurité des OIV

Règles générales communes (loi de programmation militaire)	Règles organisationnelles / de gouvernance communes (décrets d'applications)	Règles techniques communes (décrets d'application)
→ **Mise en place de systèmes de détection des incidents qualifiés par l'ANSSI** ; → **Notification sans délai des incidents** affectant les SIIV ; → **Soumission à des contrôles par l'ANSSI** ; → **Sanctions pénales**.	→ **Détermination des SIIV** par analyse d'impact ; → **Mise a jour annuelle de la liste des SIIV** (et communication à l'ANSSI) ; → **Désignation d'un représentant auprès de l'ANSSI** ; → **Mise en œuvre d'une politique de sécurité des systèmes d'information**.	→ **Homologation de sécurité des SIIV** ; → **Cartographie des éléments composant les SIIV** ; → **Procédure de maintien en conditions de sécurité des SIIV** ; → **Système de journalisation sur les SIIV et conservation pendant au moins 6 mois** ; → **Mise en place d'un SOC ou SIEM** ; → **Contrôle d'accès et authentification stricte** ; → **Cloisonnement des SIIV** ; → **Gestion stricte des supports amovibles** ; → **Indicateurs de monitoring du maintien en condition de sécurité**.

07 Du cote de la France - les obligations de sécurité des OSE & FSN

Obligations des OSE	Obligations des FSN
→ **Désignation d'un représentant auprès de l'ANSSI** ;	→ **Désignation d'un représentant dans un des pays de l'UE, ou national auprès de l'ANSSI** ;
→ **Etablissement et maintien à jour de la liste des réseaux et SI nécessaires à la fourniture des services essentiels** ;	→ **Etablissement et maintien a jour de la liste des réseaux et SI nécessaires à la fourniture des services** ;
→ **Elaboration et mise en œuvre d'une politique de sécurité** ;	→ **Elaboration et mise en œuvre d'une politique de sécurité** ;
→ **Homologation de sécurité** ;	→ **Cartographie des SI** ;
→ **Sécurité de l'architecture et de l'administration** des réseaux et SI ;	→ **Mesures de sécurité physique et environnementale** des réseaux et SI ;
→ **Contrôle des accès** ;	→ **Sécurité de l'approvisionnement des produits indispensables à la fourniture des services** ;
→ **Détection et traitement des incidents de sécurité** ;	→ **Notification sans délai à l'ANSSI des incidents** ;
→ **Notification sans délai à l'ANSSI des incidents** ;	→ **Soumission à des contrôles par l'ANSSI** ;
→ **Gestion de crise en cas d'incidents de sécurité** ;	→ **Sanction pénale des dirigeants**.
→ **Soumission aux contrôles par l'ANSSI** ;	
→ **Sanction pénale des dirigeants**.	

08 En bref

→ Si les OIV, OSE et FSN sont comparables aux CIIOs,

→ Il n'y a pas d'équivalent en France (ou sous les règlementations européennes) des Network Operators.

Le champs d'application de la CSL (chinoise) est donc beaucoup plus large, en ce qu'il capture tous les types d'entités, petites ou grandes, ayant des activités considérées comme stratégiques ou non.

09 Activités réservées & accès aux codes sources France - Chine

Activités réservées

→ **Chine** :
- ✓ **Liste négative - activités interdites ou possibilités réduites pour les étrangers / sociétés étrangères** ;
- ✓ **Contrôle de sécurité nécessaire pour les investissements étrangers** qui influent ou pourraient avoir un impact sur la sécurité nationale.

→ **France** :
- ✓ **Système d'autorisation des investissements étrangers pour les activités de nature à porter atteinte à l'ordre public, à la sécurité publique ou aux intérêts de la défense nationale**,

→ **Europe** :
- ✓ **Règlement du 19 mars 2019 établissant un cadre pour le filtrage, par les États membres, des investissements directs étrangers dans l'UE pour des motifs de sécurité ou d'ordre public**.

Produits & services homologués

→ **Chine** :
- ✓ **Contrôle de sécurité nécessaire pour les produits et services de technologie de l'information** qui influent ou pourraient avoir un impact sur la sécurité nationale ;
- ✓ **Examen de sécurité des produits et services de réseau achetés par les CIIOs** pouvant affectant la sécurité nationale ;
- ✓ Equipements de réseau critiques et les produits spécialisés de sécurité des réseaux: **certifiés conformes** aux normes et standards nationaux.

→ **France**:
- ✓ **Systèmes de détection et prestataires de service exploitant ces systèmes, qualifiés par l'ANSSI pour les OIV**.

→ **Europe**:
- ✓ Résolution du Parlement européen du 12 mars 2019 sur les menaces pour la sécurité liées à la présence technologique croissante de la Chine.

10 Données personnelles - similarités & différences

- → Collecte et utilisation soumises aux principes de **légalité, de légitimité et de nécessité** ;
- → **Obligation d'information des personnes concernées** :
- → **Consentement nécessaire** ;
- → **Droit des personnes** :
  - Information ;
  - correction des données ;
  - Intervention d'une personne en cas de décision automatique ;
  - Réponse au demande et plaintes ;
  - suppression des données dans certaines circonstances ;
- → **Interdiction du traitement ultérieur** ;
- → **Obligation de mettre en place des mesures techniques et organisationnelles pour assurer la sécurité des données** ;
- → **Anonymisation & pseudonimisation** ;
- → **Minimisation des données** ;
- → **Systèmes de requêtes et plaintes** ;
- → **DPO** ;

- → **Notification des violations de données** aux personnes concernées et à l'autorité de réglementation compétente ;
- → **Transferts internationaux soumis au consentement et à une évaluation de sécurité (et autorisation)** :
  - **Des la 1ere donnée personnelle** ;
  - Et les données importantes ;
- → **Déclaration préalable et approbation nécessaire pour les transferts internationaux de données sensibles et données importantes**.

11 Les données importantes de la Chine

→ Les « **données importantes** » :

- les données qui, **si elles sont divulguées, peuvent affecter directement la sécurité nationale, la sécurité économique, l'intérêt public, la stabilité sociale ou la santé et la sécurité publiques de la Chine** ;
- un grand volume de données relatives à la population, à la génétique, aux soins de santé ou aux ressources géographiques et minérales, à l'exclusion des données administratives, opérationnelles et internes des entreprises et des données personnelles ;
- Les données relative à la cybersécurité.

TEKID

www.tek-id.com

INTELLIGENCE / TECHNOLOGY / INNOVATION /
INVESTIGATION / COMPLIANCE

contact@tek-id.com

BILALIAN
avocatsassociés

www.bilalian-avocats.com.com

mail@bilalian-avocats.com