CentraleSupélec

Mastère Spécialisé® Ingénierie des Systèmes Informatiques Ouverts

Fondamentaux : Sécurité des systèmes d'information

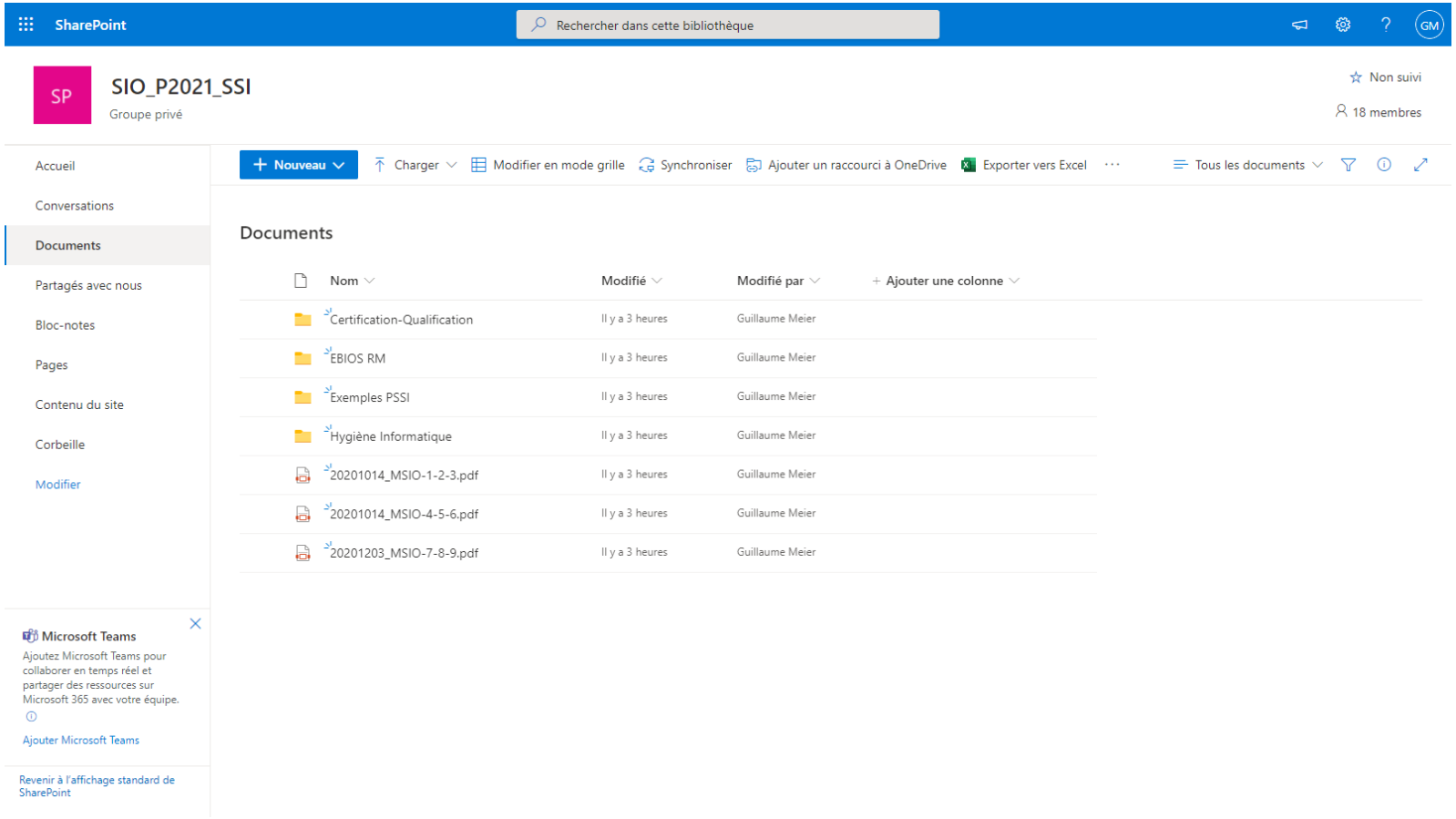
CentraleSupélec

Agenda du module Sécurité des SI

- 14/10/2020 : session 1, 2, 3
  - Les enjeux de la sécurité des S.I.
  - Les besoins de sécurité
  - Notions de vulnérabilité, menace, attaque
  - Panorama de quelques menaces
  - Le droit des T.I.C. et l'organisation de la sécurité en France
- 28/10/2020 : session 4, 5, 6
  - Analyse de risque – EBIOS Risk Manager
- 02/12/2020 : session 7, 8, 9
  - Intégrer la sécurité au sein d'une organisation
  - Intégrer la sécurité dans les projets
  - Difficultés liées à la prise en compte de la sécurité
- 17/12/2020 : session 10, 11, 12 et évaluation
  - Homologation
  - RGPD

Espace SIO_P2021_SSI

- Documents disponibles
  - https://centralesupelec.sharepoint.com/sites/SIO_P2021_SSI/Documents%20partages/Forms/AllItems.aspx



CentraleSupélec

CentraleSupélec

1. Homologation

a. Préambule
b. Étape 1
c. Étape 2
d. Étape 3
e. Étape 4
f. Étape 5
g. Étape 6
h. Étape 7
i. Étape 8
j. Étape 9
k. Conseils pour réussir

1. Homologation de sécurité

a. Préambule

Pourquoi l'homologation de sécurité ?

- *Emménagement dans un établissement*
  - *Conformité à la réglementation,*
  - *Sécurité des biens et des personnes*
  - *Certifications, Label du bâtiment*

Terme « homologation » recouvre deux notions distinctes

- Homologation de sécurité
  - permet à un responsable d'attester la maîtrise des risques
- Démarche d'homologation
  - préalable à l'instauration de la confiance dans les systèmes d'information et dans leur exploitation.
  - rendue obligatoire par des textes IGI n°1300, RGS, PSSIE

1. Homologation de sécurité

a. Préambule

Qu'est-ce qu'une homologation de sécurité ?

L'objectif de la ***démarche d'homologation*** d'un système d'information (SI) est :

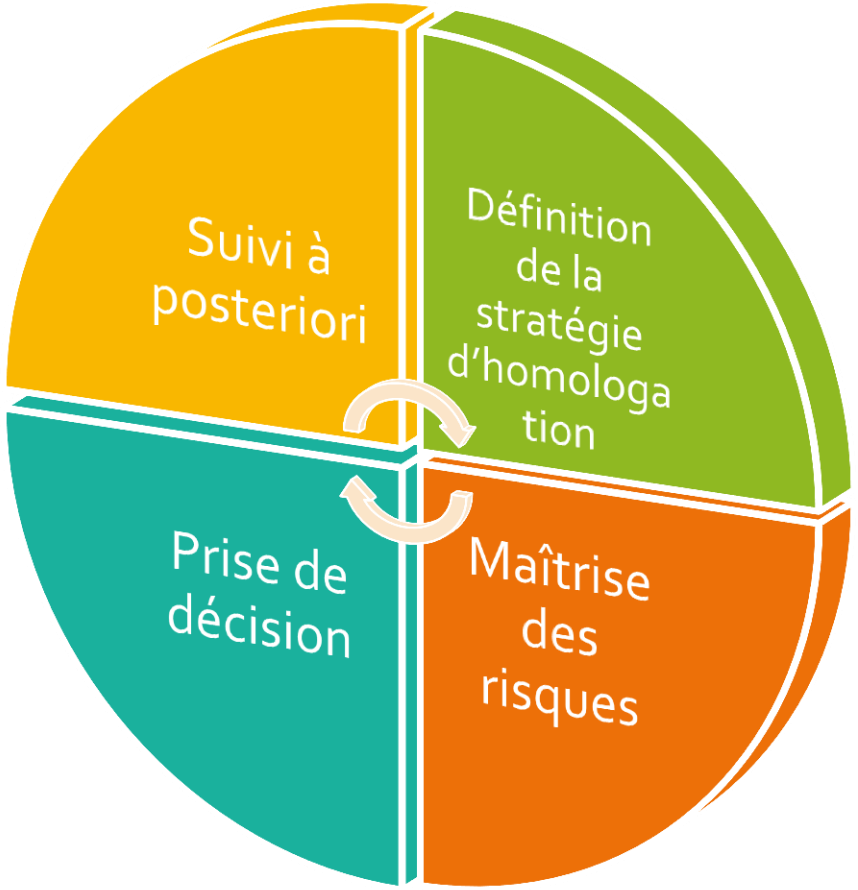
- de trouver un équilibre entre le risque acceptable et les coûts de sécurisation,
- puis de faire arbitrer cet équilibre, de **manière formelle**, par un responsable qui a autorité pour le faire.

- Doit s'intégrer dans le cycle de vie du système d'information.

1. Homologation de sécurité

a. Préambule

Comment homologuer un système d'information ?



CentraleSupélec

1. Homologation de sécurité

a. Préambule

Définition de la stratégie d'homologation

- Étape n° 1 : Quel système d'information dois-je homologuer et pourquoi ?
  - Définir le référentiel réglementaire applicable et délimiter le périmètre du système à homologuer.
- Étape n° 2 : Quel type de démarche dois-je mettre en œuvre ?
  - Estimer les enjeux de sécurité du système et en déduire la profondeur nécessaire de la démarche à mettre en œuvre.
- Étape n° 3 : Qui contribue à la démarche ?
  - Identifier les acteurs de l'homologation et leur rôle (décisionnaire, assistance, expertise technique, etc.).
- Étape n° 4 : Comment s'organise-t-on pour recueillir et présenter les informations ?
  - Détailler le contenu du dossier d'homologation et définir le planning.

CentraleSupélec

1. Homologation de sécurité

a. Préambule

Maîtrise des risques

- Étape n° 5 : Quels sont les risques pesant sur le système ?
  - Analyser les risques pesant sur le système en fonction du contexte et de la nature de l'organisme et fixer les objectifs de sécurité.
- Étape n° 6 : La réalité correspond-elle à l'analyse ?
  - Mesurer l'écart entre les objectifs et la réalité.
- Étape n° 7 : Quelles sont les mesures de sécurité supplémentaires à mettre en œuvre pour couvrir ces risques ?
  - Analyser et mettre en œuvre les mesures nécessaires à la réduction des risques pesant sur le système d'information. Identifier les risques résiduels.

CentraleSupélec

1. Homologation de sécurité

a. Préambule

Prise de décision

- Étape no 8 : Comment réaliser la décision d'homologation ?
  - Accepter les risques résiduels : l'autorité d'homologation signe une attestation formelle autorisant la mise en service du système d'information, du point de vue de la sécurité.

Suivi a posteriori

- Étape no 9 : Qu'est-il prévu pour maintenir la sécurité et continuer de l'améliorer ?
  - Mettre en place une procédure de révision périodique de l'homologation et un plan d'action pour traiter les risques résiduels et les nouveaux risques qui apparaîtraient.

CentraleSupélec

1. Homologation de sécurité

b. Étape 1

Quel système d'information dois-je homologuer et pourquoi ?

1 . Préciser le référentiel réglementaire

- Obligatoire
  - **l'instruction générale interministérielle no 1300** (IGI 1300), pour les systèmes traitant d'informations classifiées de défense ;
  - **le référentiel général de sécurité** (RGS), pour les systèmes permettant des échanges entre une autorité administrative et les usagers ou entre autorités administratives ;
  - **la politique de sécurité des systèmes d'information de l'État** (PSSIE), pour les systèmes des administrations de l'État.
- Recommandé dans tous les autres cas

2 . Délimiter le périmètre du système

- éléments fonctionnels et d'organisation
- éléments techniques
- périmètre géographique et physique

CentraleSupélec

1. Homologation de sécurité

c. Étape 2

Quel type de démarche dois-je mettre en œuvre ?

1 . Autodiagnostiquer les besoins de sécurité du système et le niveau de maturité SSI de l'organisme

- déterminer si le besoin de sécurité du système
  - nul, faible, moyen ou fort.
- déterminer le niveau de maturité SSI de l'organisme
  - élémentaire, moyenne ou avancée

CentraleSupélec

1. Homologation de sécurité

c. Étape 2

2 . En déduire la démarche appropriée

		Besoin de sécurité du Système		
		Faible	Moyen	Fort
Niveau SSI de l'organisme	élémentaire	**Pianissimo :** démarche autonome a minima	**Mezzo Forte :** démarche assistée approfondie	**Mezzo Forte :** démarche assistée approfondie
	moyen	**Pianissimo :** démarche autonome a minima	**Mezzo Piano :** démarche autonome approfondie	**Mezzo Forte :** démarche assistée approfondie
	avancé	**Pianissimo :** démarche autonome a minima	**Forte :** Démarche spécifique	**Forte :** Démarche spécifique

1. Homologation de sécurité

d. Étape 3

Qui contribue à la démarche ?

1 . L'autorité d'homologation (AH)

- Personne physique qui
  - prononce l'homologation de sécurité du système d'information,
  - prend la décision d'accepter les risques résiduels identifiés sur le système.
- doit être désignée à un niveau hiérarchique suffisant pour assumer toutes les responsabilités
  - se situe à un niveau de direction dans l'organisme.

2 . La commission d'homologation

- assiste l'autorité d'homologation pour l'instruction de l'homologation
- est chargée de préparer la décision d'homologation.
- réunit les responsables métier concernés par le service à homologuer et des experts techniques.
  - taille et la composition adaptés à la nature du système et proportionnées à ses enjeux.
- chargée
  - du suivi des *plannings*,
  - de l'analyse de l'ensemble des documents versés au dossier d'homologation.
- se prononce sur la pertinence des livrables et peut les valider

CentraleSupélec

1. Homologation de sécurité

d. Étape 3

3 . Les acteurs de l'homologation

- La maîtrise d'ouvrage
- Le RSSI
- Le responsable d'exploitation du système
- Les prestataires

- Les systèmes interconnectés

CentraleSupélec

1. Homologation de sécurité

e. Étape 4

1 . Le contenu du dossier d'homologation

	Pianissimo	Mezzo Piano	Mezzo Forte	Forte
Stratégie d'homologation	Indispensable			
Référentiel de sécurité	Si existant			Indispensable
Document présentant les risques identifies et les objectifs de sécurité	Indispensable			
Politique de sécurité des systèmes d'information	Recommandé	Fortement recommandé		Indispensable
Procédure d'exploitation sécurisée du système	Indispensable			
Journal de bord de l'homologation	Recommandé	Fortement recommandé		Indispensable
Certificats de qualification des produits ou prestataires	Si existant			Indispensable
Résultats d'audits	Si existant	Recommandé	Fortement recommandé	Indispensable
Liste des risques résiduels	Indispensable			
Décision d'homologation	Indispensable			
Spécifiquement pour les systèmes déjà en services:				
Tableau de bord des incidents et de leur résolution	Recommandé	Fortement recommandé	Indispensable	Indispensable
Résultats d'audits intermédiaires	Si existant	Recommandé		Indispensable
Journal des évolutions du système	Si existant			Indispensable

1. Homologation de sécurité

e. Étape 4

2 . Planning de l'homologation

- directement dépendant du calendrier du projet
- La démarche visant à l'homologation
  - doit être lancée en amont
  - être totalement intégrée au projet dès les phases d'étude et de conception
- Les principales étapes de l'homologation sont fixées dans la stratégie d'homologation.
- L'Homologation doit être prononcée préalablement à la mise en service opérationnelle du SI
- 2 temps forts :
  - construction du référentiel documentaire et l'analyse de risque
  - déploiement, l'audit, l'homologation et la mise en service opérationnel

CentraleSupélec

1. Homologation de sécurité

f. Étape 5

Quels sont les risques pesant sur le système ?

1 . L'analyse de risque

- Mesure de l'importance du risque
  - combinaison de la gravité et de la vraisemblance
- Réaliser une analyse EBIOS Risk Manager

2 . Identifier les mesures de sécurité

- Principe de base et hygiène
  - le guide des 42 règles d'hygiène informatique ;
  - le guide d'externalisation pour les systèmes d'information ;
  - Guides et notes techniques, notamment celle sur la sécurité web…
- Référentiels de sécurité normatifs et réglementaires
  - ISO 27002
  - Directive NIS, RGS, II 901, IGI 1300…
- À l'issue de l'analyse de risque – Atelier 5
  - les mesures de sécurité permettant de couvrir les risques identifiés
  - **Reste les *risques résiduels* qui doivent être acceptés dans le cadre de l'homologation.**

1. Homologation de sécurité

g. Étape 6

La réalité correspond-elle à l'analyse ?

1 . Réalisation du contrôle

	Pianissimo	Mezzo Piano	Mezzo Forte	Forte
Audits	Optionnel	Recommandé sur les segments les moins maîtrisés	Fortement recommandé	Indispensable

2 . Définition du périmètre du contrôle

- audit dont le périmètre est délimité par l'AH.
  - code source, configuration des équipements, architecture du système, organisation mise en place, etc.
  - Potentiellement selon le référentiel et par un prestataire qualifié PASSI
- Des tests d'intrusions peuvent être effectués

3 . Conséquences de l'audit sur le dossier d'homologation

- Rapport d'audit écrit
  - doit faire apparaître :
    - une évolution des menaces sur le système ;
    - la découverte éventuelle de nouvelles vulnérabilités ;
    - La préconisation de mesures correctrices, le cas échéant.
  - intégré au dossier d'homologation,
- Mise à jour du dossier d'homologation en tenant compte des nouveaux risques

1. Homologation de sécurité

h. Étape 7

Quelles sont les mesures de sécurité supplémentaires pour couvrir les risques ?

- Rappel Atelier 5 EBIOS RM
  - A. Réaliser la synthèse des scénarios de risque
  - B. Définir la stratégie de traitement du risque et les mesures de sécurité
  - **C. Évaluer et documenter les risques résiduels**
  - **D. Mette en place le cadre de suivi des risques**

1 . Le traitement du risque

- l'AH se prononce formellement sur l'ensemble des risques résiduels

2 . La mise en œuvre de mesures de sécurité

- de nature technique, organisationnelle ou juridique.
- décidées par l'AH sur proposition de la commission d'homologation.

3 . Définition du plan d'action

- Mise en place du comité de pilotage pour assurer le suivi des risques
  - Suivi de l'avancement du PACS (plan d'amélioration continue de la sécurité)
  - Suivi des indicateurs de MCS
  - Suivi des mises à jour de l'étude de risques selon les cycles stratégique et opérationnel

CentraleSupélec

1. Homologation de sécurité

i. Étape 8

Comment réaliser la décision d'homologation ?

1 . Le périmètre de l'homologation

- A minima tiens compte des éléments suivants :
  - référentiel réglementaire ;
  - références des pièces du dossier d'homologation ;
  - périmètre géographique et physique (localisations géographiques, locaux, etc.) ;
  - périmètre fonctionnel et organisationnel (fonctionnalités, types d'informations traitées par le système et sensibilité, types d'utilisateurs, règles d'emploi, procédures, conditions d'emploi des produits de sécurité, etc.) ;
  - périmètre technique (cartographie, architecture détaillée du système, produits certifiés/qualifiés/agréés, prestataires qualifiés, etc.).

2 . Les conditions accompagnant l'homologation

- En fonction des risques résiduels identifiés
  - conditions d'exploitation
  - PACS visant à maintenir et à améliorer le niveau de sécurité du SI
- À chaque action, le PACS associe
  - une personne pilote
  - une échéance

1. Homologation de sécurité

i. Étape 8

3 . La durée de l'homologation

	Durée maximale recommandée
SI maîtrisé Peu de risques résiduels	5 ans avec revue annuelle
SI maîtrisé De nombreux risques résiduels	3 ans avec revue annuelle
SI non maîtrisé De nombreux risques résiduels	1 an

4 . Conditions de suspension ou de retrait de l'homologation

- Validité de l'homologation tant que le SI est exploité dans le contexte décrit dans le dossier d'homologation.
- Réexamen du dossier nécessaire pour les changements suivant :
  - raccordement d'un nouveau site sur le système d'information
  - ajout d'une fonctionnalité majeure ou succession de modifications mineures
  - réduction de l'effectif affecté à une tâche impactant la sécurité
  - changement d'un ou de plusieurs prestataires
  - non-respect d'au moins une des conditions de l'homologation
  - changement du niveau de sensibilité des informations traitées et, plus généralement, du niveau du risque
  - évolution du statut de l'homologation des systèmes interconnectés
  - publication d'incidents de nature à remettre en cause les garanties recueillies dans le dossier de sécurité
  - décision de l'autorité d'homologation
  - prise de fonction d'une nouvelle autorité d'homologation
- L'AH réuni annuellement la commission d'homologation pour la revue du respect des conditions de l'homologation

CentraleSupélec

1. Homologation de sécurité

j. Étape 9

Qu'est-il prévu pour continuer d'améliorer la sécurité ?

1 . Suivi de l'homologation

- L'AH doit veiller au maintien du niveau de sécurité du système.
- La commission d'homologation réalise annuellement un suivi de l'homologation.
  - doit donc rester simple et se limiter à une mise à jour du dossier
  - analyse succincte des évolutions et des incidents intervenus au cours de l'année
- En préparation du renouvellement de l'homologation,
  - Mise à jour régulière du dossier d'homologation par
    - éventuelles analyses de vulnérabilités
    - les comptes rendus de contrôle
    - les rapports d'audits complémentaires.
- Réunion périodique de la commission d'homologation
  - vérifier que les conditions d'homologation sont toujours respectées
  - évite de reprendre l'homologation à zéro au terme de sa durée de validité

CentraleSupélec

1. Homologation de sécurité

j. Étape 9

Qu'est-il prévu pour continuer d'améliorer la sécurité ?

2 . Maintien en conditions de sécurité

- Respect dans le temps des conditions de l'homologation
- Veille technologique permettant d'identifier les nouvelles vulnérabilités
- Assurer la correction des vulnérabilités
- vérifier :
  - les clauses de sécurité et de MCS du système et des prestataires
  - les capacités d'évolution et d'interopérabilité du SI (MCO)

CentraleSupélec

1. Homologation de sécurité

k. Conseils pour réussir

Pour réussir une démarche d'homologation

- Débuter suffisamment tôt la démarche d'homologation
- Prévoir une validation formelle des décisions au bon niveau hiérarchique
- Désigner un véritable chef de projet
  - disponible tout au long du projet
- Maîtriser le calendrier
  - ne pas être trop contraint par des nécessités opérationnelles
- Bien définir le périmètre
  - disposer d'une architecture précise du système
  - prendre en compte les interconnexions éventuelles
- S'appuyer sur des documents écrits, explicites, sans ambiguïté
  - évite les quiproquos entre les parties prenantes au projet
- Sensibilisation des acteurs
  - à la démarche d'homologation
  - à EBIOS Risk Manager

2. RGPD

a. Définitions
b. RGPD / GDPR
c. Une nouvelle logique de responsabilité
d. Droits des personnes renforcés
e. Risque aggravé de sanctions
f. DPD / DPO
g. Documentation CNIL

2. RGPD

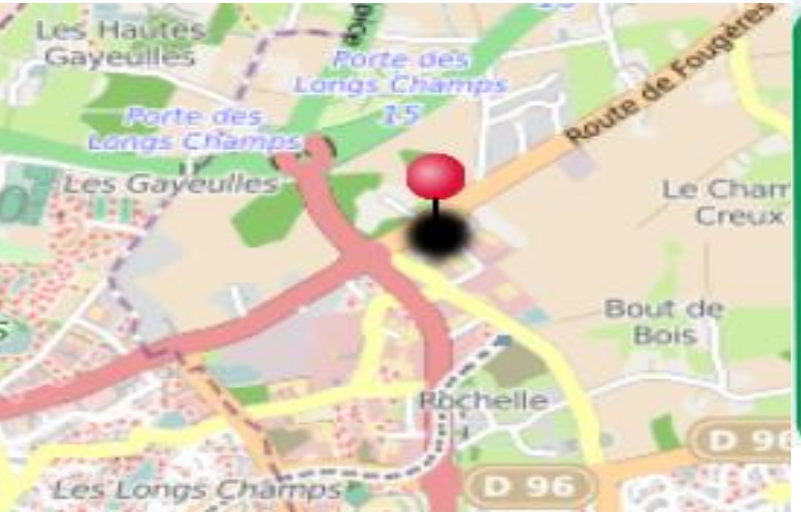
a. Définitions

- Données à caractère personnel :
  Constitue une donnée à caractère personnel toute information se rapportant à une personne physique identifiée ou identifiable :
  - Directement ou
  - Indirectement, notamment par référence :

- à un identifiant, tel que :
  - un nom
  - un numéro d'identification
  - des données de localisation
  - un identifiant en ligne

- à un ou plusieurs éléments spécifiques propres à son identité
  - physique, physiologique, génétique, psychique
  - économique, culturelle ou sociale

- Loi Informatique et Libertés (LIL) vs Règlement général pour la protection des données (RGPD) :
  - définition élargie et plus précise par rapport à la LIL

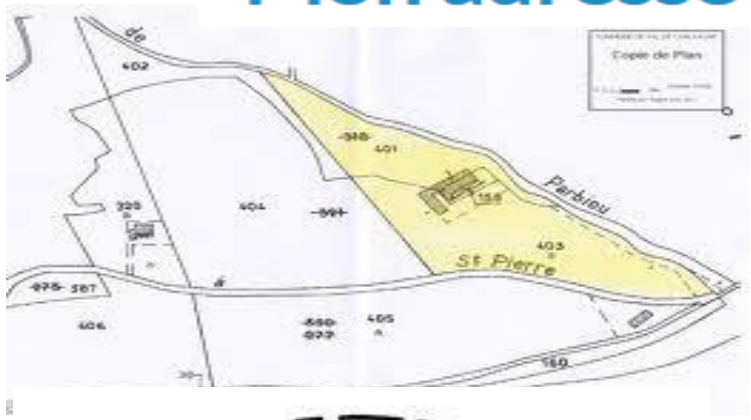


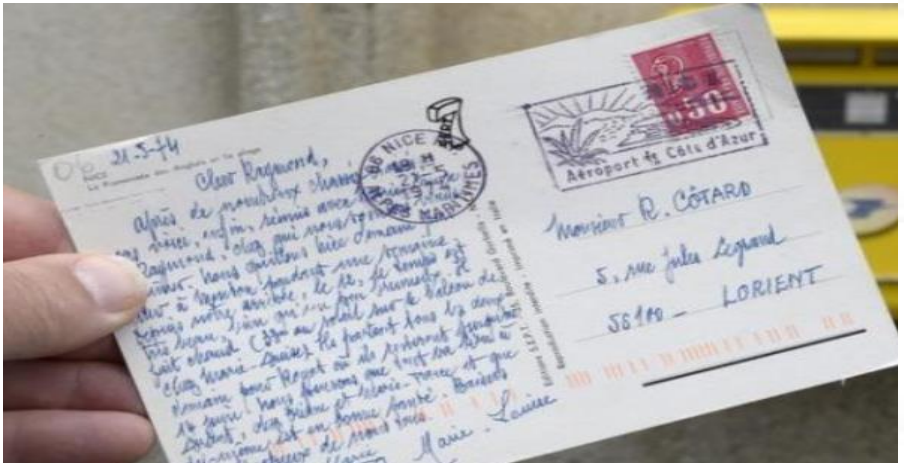
+33 0 42 99 96 66

Mon adresse ip : *37.58.187.57*

Arthur

25.01.2019





mail.man@mondomaine.fr

2. RGPD

a. Définitions

- Traitement :
  Constitue un traitement de données à caractère personnel :
  - toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que

- la collecte
- l'enregistrement
- l'organisation, la structuration,
- la conservation
- l'adaptation ou la modification
- l'extraction, la consultation l'utilisation
- la communication par transmission, la diffusion ou toute autre forme de mise à disposition
- le rapprochement ou l'interconnexion,
- la limitation
- l'effacement ou la destruction

- LIL vs RGPD : définition peu modifiée par rapport à la LIL

RECENSEMENT DE LA POPULATION

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

AVIS D'IMPOSITIO
TAXES FONCIÈRES
es et perçues par la commune, le dépar
la région et divers organismes

2. RGPD

a. Définitions

- Fichier :
  Constitue un fichier de données à caractère personnel :
  - tout ensemble structuré et stable de données à caractère personnel
  - accessibles selon des critères déterminés, que cet ensemble soit :
    - centralisé
    - décentralisé ou
    - réparti de manière fonctionnelle ou géographique

2. RGPD

a. Définitions

- Acteurs:
- Le responsable du traitement (RT) :
  - Définition (Art 4):
- La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.
  - La personne dont la responsabilité civile et pénale peut être engagée
- Pas de changement dans la définition et la conception du responsable de traitement par rapport à la LIL

2. RGPD

a. Définitions

Les grands principes de la collecte de données

- **Principe de finalité** : indiquer à quoi le fichier va servir.
  - Les données ne peuvent être recueillies que pour une finalité :
    - Déterminée, explicite et légitime
    - Correspondant aux missions de l'organisme

→ Autrement dit, ce principe limite la manière dont le responsable du traitement pourra utiliser ou réutiliser ces données dans le futur.

- **Principe de pertinence** : aussi appelé principe de proportionnalité ou de minimisation de la collecte.
  - Seules les données strictement nécessaires à la réalisation de l'objectif peuvent être collectées.

- **Principe de temporalité** : aussi appelé principe de conservation.
  - Une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de conserver les données et elles doivent être supprimées.

2. RGPD

a. Définitions

Les autres grands principes de la LIL

- Sécurité des fichiers
  - Obligation de prendre toutes les mesures nécessaires pour :
    - Garantir la sécurité des données collectées
    - Garantir leur confidentialité
  - Obligation d'adapter ces mesures en fonction des risques qui pèsent sur les données

- Information des personnes de leurs droits :
  - Droit d'accéder à ses données
  - Droit de les rectifier
  - Droit de s'opposer à leur utilisation

- Formalités préalables auprès de la CNIL
  - Déclaration normale
  - Demande d'autorisation
  - Demande d'avis
  - Simplifications

2. RGPD

b. RGPD

- La Loi informatique et Libertés : en vigueur depuis le 6 janvier 1978
  - Lien : ICI

- Le Règlement général sur la protection des données (RGPD) : en vigueur à partir du 25 mai 2018.
  - Lien : ICI

RGPD

aussi appelé GDPR en anglais

2. RGPD

b. RGPD

- Un long processus :
  - 4 ans de négociation, 4 000 amendements, 88 pages
  - Adopté le 27 avril 2016
  - Publié au JOUE le 4 juin 2016
  - Entrée en application des dispositions : 25 mai 2018

- Constat :
  - Manque d'harmonisation entre les niveaux de protection au sein de l'UE
  - Évolution rapide des technologies
  - De plus en plus de données collectées
  - Nécessité de susciter ou maintenir la confiance

- Des renvois aux droits nationaux :
  - 56 cas où les États Membres gardent leur pouvoir , notamment :
    - santé, NIR, emploi,
    - exécution d'une mission d'intérêt publique ou exercice de l'autorité publique,
    - archivage, statistiques, recherche scientifiques, recherche historique
  - Loi informatique et libertés 2 en attente

2. RGPD

b. RGPD

Ce qui change :

- Une nouvelle logique de responsabilité
- Les droits des personnes renforcés
- Un risque aggravé de sanctions
- Un Délégué à la Protection des Données (DPD) obligatoire

2. RGPD

c. Une nouvelle logique de responsabilité

- Réflexion sur la protection des données dès la création / conception d'un service : « Privacy by design » :
  - Dès la conception d'un service et par défaut
  - Mise en œuvre de mesures techniques et / organisationnelles
  - Veiller à limiter la quantité de données traitées

- Suppression des obligations de déclarations préalables pour les traitements sans risque pour la vie privée
  - Logique de responsabilisation des RT
  - Obligations de mettre en place des mesures de protection, de les documenter et de démontrer la conformité à tout moment (mise en conformité dynamique et permanente)
  - Maintien des déclarations préalables pour les demandes d'autorisation

CentraleSupélec

2. RGPD

c. Une nouvelle logique de responsabilité

- Etudes d'impact sur la vie privée (EIVP) obligatoires :
  - pour les traitements « à risques », traitant des données sensibles ou reposant sur du profilage
  - pour faire apparaître les caractéristiques du traitement, les risques et les mesures adoptées pour protéger les données
  - Documentation CNIL sur les EIVP : ICI
  - Aussi appelé « PIA » pour Privacy Impact Assessment en anglais
- Partage des responsabilités : le sous-traitant aussi doit respecter le RGPD
  - Potentielle co-responsabilité
  - Obligation de désigner un DPD et de tenir un registre des traitements
  - Obligation de conseil pour permettre la conformité au RGPD (EIVP, failles de sécurité, audit, destruction des données)

2. RGPD

d. Droits des personnes renforcés

- Obligation d'information dans des termes clairs
  - L'information doit être claire, intelligible et facilement accessible
  - Les personnes doivent donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer, de façon « non ambigüe »
  - La charge de la preuve pèse sur le responsable du traitement

- Obligation d'information en cas de perte de données :
  - Obligation d'informer la CNIL dans les 72 heures
  - Obligation d'informer les personnes concernées si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes
  - Droit à réparation du préjudice, auprès du RT ou de son sous-traitant

- Délais pour faire droit à une demande : « dans les meilleurs délais » et au plus tard en 1 mois

2. RGPD

e. Risque aggravé de sanctions

- Le RT et le sous-traitant peuvent faire l'objet de sanctions administratives : jusqu'à 20 millions d'euros pour le responsable du traitement et de 2 à 4 % du chiffre d'affaires annuels du sous-traitant

- Des sanctions pénales toujours en vigueur :
  - Article L226-16 à L226-24 et articles R625-10 à R625-13 du code pénal
  - Peine d'amendes à peines de prison avec sursis

- En cas de non-conformité, le risque est ailleurs : réputation, image, perte de confiance, climat social

- Loi République numérique et loi Informatiques et Libertés 2 pour adapter précisions en droit français
  - https://www.cnil.fr/fr/sanctions-2250000-euros-et-800000-euros-pour-carrefour-france-carrefour-banque
  - https://www.cnil.fr/fr/cookies-sanction-de-35-millions-deuros-lencontre-damazon-europe-core
  - https://www.cnil.fr/fr/cookies-sanction-de-60-millions-deuros-lencontre-de-google-llc-et-de-40-millions-deuros-lencontre-de

2. RGPD

f. DPD / DPO

- Désignation obligatoire du délégué à la protection des données (DPD ou DPO en anglais), sans seuil de dispense.

- Profil :
  - Doit être qualifié : qualités professionnelles, connaissances spécialisées du droit et des pratiques en matière de protection de données
  - Doit bénéficier d'actions de formation continue

- Obligations pour l'organisme de :
  - fournir au DPD les ressources nécessaires à ses missions
  - l'associer d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données
  - lui donner accès aux données
  - lui permettre de se former

2. RGPD

f. DPD / DPO

- Informer, conseiller et accompagner, afin de faire respecter le règlement européen et le droit national dans son organisme
- Sensibiliser aux enjeux de la protection des données personnelles
- Superviser des audits internes sur la protection des données personnelles
- Conseiller le responsable sur l'opportunité de réaliser une analyse d'impact sur la vie privée (EIVP) et d'en vérifier l'exécution
- Recevoir les réclamations relatives à la protection des données et y répondre
- Coopérer avec la CNIL et être son point de contact dans l'organisme
- Tenir le registre des traitements et dresser le bilan annuel
- → Missions élargies par rapport au CIL : plus grandes responsabilités !

2017 CentraleSupélec

2. RGPD

f. DPD / DPO

CIL vs Délégué à la protection des données 2018

- Le CIL : Correspondant informatique et libertés

- Il diffuse la culture « Informatique et Libertés » et instaure des bonnes pratiques dans l'organisme.
- Il est l'interlocuteur de la CNIL au sein de l'organisme et veille au respect de la loi Informatique et Libertés. Il sensibilise les agents, la direction et les élus.
- Il tient des registres de traitement et dresse un bilan annuel de ses activités
- Sa désignation était facultative jusqu'à présent

- Le DPD : Délégué à la Protection des Données ou Data Protection Officer (DPO)

- **Informer, conseiller et accompagner** au sein de sa structure, afin de faire respecter le règlement européen et le droit national en matière de protection des données personnelles
- **Sensibiliser** au sein de sa structure aux enjeux de la protection des données personnelles
- Superviser des **audits internes** sur la protection des données personnelles
- Conseiller le responsable sur l'opportunité de réaliser une **analyse d'impact sur la vie privée** (EIVP) et d'en vérifier l'exécution
- Recevoir les **réclamations** relatives à la protection des données et y répondre
- **Coopérer avec l'autorité de contrôle** (la CNIL) et être son point de contact au sein de sa structure

CentraleSupélec

2. RGPD

f. DPD / DPO

- Possibilité de :
  - Externaliser un DPD : avocat, prestataire
  - Mutualiser un DPD : à l'échelle d'un organisme, à l'échelle d'un département, etc.
    - Mutualiser pour éviter le conflit d'intérêt : DG ≠ DPD
    - Mutualiser pour disposer
      - des ressources nécessaires
      - d'un DPD formé et habitué aux problématiques de protection des données
      - d'un DPD indépendant

2.RGPD

g. Documentation CNIL

- Règlement européen du 23 mai 2018 :
  - https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- https://www.cnil.fr/fr/comprendre-le-rgpd
- Règlement européen : se préparer en 6 étapes
  - https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes
  - https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf
- En quoi les collectivités territoriales sont-elles impactées par le règlement européen sur la protection des données ?
  - https://www.cnil.fr/fr/RGPD-quel-impact-pour-les-collectivi__tes-territoriales
- Devenir délégué à la protection des données :
  - https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees
- Documenter la conformité :
  - https://www.cnil.fr/fr/documenter-la-conformite

2.RGPD

g. Documentation CNIL

- Règlement européen du 23 mai 2018 :
  - https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- Comprendre le RGPD
  - https://www.cnil.fr/fr/comprendre-le-rgpd
- Devenir délégué à la protection des données :
  - https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

PASSER À L'ACTION

Les grandes étapes pour protéger les données personnelles de votre organisme

Démarrer avec le RGPD

EFFECTUER UNE DÉMARCHE

Les services en ligne pour désigner un délégué, déclarer un fichier, demander une autorisation…

Réaliser une démarche

UTILISER LES OUTILS

Registre, information des personnes, AIPD… les outils de la protection des données.

Découvrir les outils

2.RGPD

g. Documentation CNIL

- Modèle de registre simplifié:
  - https://www.cnil.fr/sites/default/files/atoms/files/registre-traitement-simplifie.ods
- Etudes d'impact sur la vie privée (PIA en anglais) :
  - PIA-1, la méthode : Comment mener une étude d'impact sur la vie privée
  - PIA-2, l'outillage : Modèles et bases de connaissances de l'étude d'impact sur la vie privée
  - PIA-3, les bonnes pratiques : Mesures pour traiter les risques sur les libertés et la vie privée
- Outil PIA v2.3.0 : téléchargez et installez le logiciel de la CNIL
  - Logiciel open source PIA facilite la conduite et la formalisation d'analyses d'impact relatives à la protection des données (AIPD) telles que prévues par le RGP
  - https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
- Le droit à la portabilité en question :
  - https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions

CentraleSupélec

3. Évaluation

3. Évaluation

a. Préambule

- L'évaluation consiste en une étude de cas sur la base du fil rouge
  - Démarche d'homologation jusqu'à la décision d'homologation
  - Analyse de risque EBIOS RM
  - Bonus RGPD : analyse d'impact sur la protection des données

- Quelques règles pour la livraison
  - Règle de nommage des fichiers :
    - <nom>_<prénom>_Description_SI.docs
    - <nom>_<prénom>_StrategieHomologation.docx
    - <nom>_<prénom>_EBIOS_RM.xlsx
    - <nom>_<prénom>_PES.xlsx
    - <nom>_<prénom>_DecisionHomologation.docx
    - <nom>_<prénom>_PIA.json

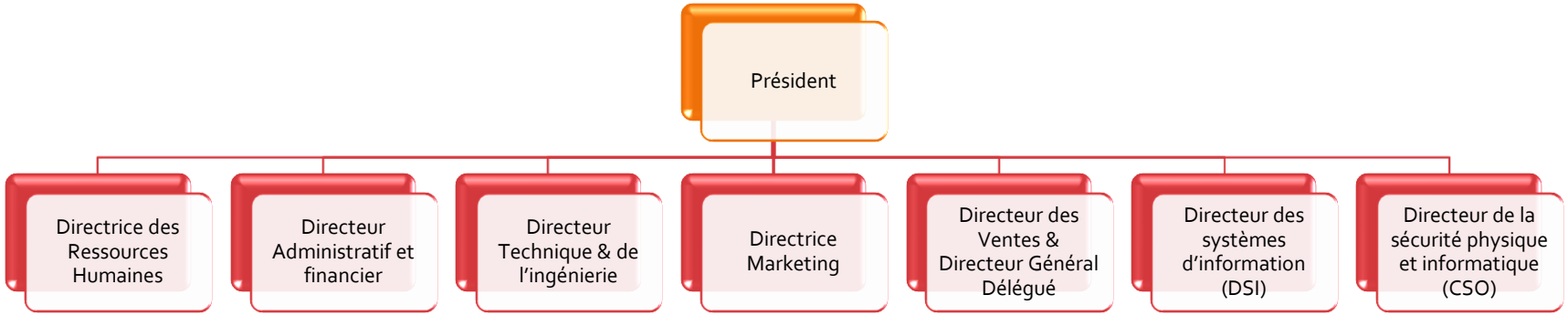
- Date de remise au plus tard : 31/01/2021

CentraleSupélec

3. Évaluation

b. Fil rouge

- Hypothèses en lien avec la réalisation du projet fil rouge :
  - Le projet est réalisé au sein du département ingénierie d'un organisme dont le niveau SSI est jugé faible et le besoin de sécurité moyen
  - Le projet consiste en la réalisation, en 6 mois, d'une application (API de type REST en Python) au sein d'un système d'information dont le serveur distant est hébergé dans le cloud chez un prestataire de confiance. Il sera livré à la DSI pour l'exploitation.
  - Les utilisateurs et leurs poste clients sont uniquement ceux de l'organisme
  - l'organisation de l'organisme est la suivante :



CentraleSupélec

3. Évaluation

c. Travaux attendus

- Décrivez succinctement le SI et son architecture, l'architecture de l'application et l'hébergement chez le prestataire cloud
  - Schéma + quelques lignes de texte => ce sera le périmètre pour l'analyse de risque et la démarche d'homologation
  - Usager du SI : Utilisateurs de l'application, télé-administrateurs de l'application et du SI.
  - Description des mesures de sécurité envisagées

- Rédaction d'une stratégie d'homologation simplifiée
  - Chapitres 1, 2 (2.1 & 2.2), 3, 4, 5 (5.1,5.4, 5.5, 5.6, 5.8, 5.9, 5.10, 5.11), 6 et 9 (9.1, 9.2, 9.3, 9.6, 9.7)
  - Désigner l'AH qui vous semble la plus pertinente et les parties prenante de la commission d'homologation

- Analyse de risque EBIOS RM
  - Renseigner le fichier Excel « EBIOS Risk Manager Tools FR.xlsx »
  - Atelier 1 - Socle de sécurité : guide d'hygiène
  - Atelier 2 - 2 couples SR/OV
  - Atelier 3 – au moins une PP & 2 scénario stratégiques
    - fournisseur infra Cloud : maturité SSI bonne et prestataire de confiance
  - Atelier 4 – élaborer les scénarios opérationnels pour 1 scénario stratégique
  - Atelier 5 – renseigner
    - au moins 2 risques et une mesure de réduction d'un risques,
    - une fiche de risque résiduel qui devra être approuvée par l'autorité d'homologation
    - Le plan d'amélioration continue de la sécurité

- Rédaction des Procédures d'exploitation sécurisée du système
  - Uniquement chapitre 5 et 6 en pensant à bien identifié les responsabilités d'exploitation du prestataire Cloud et de l'organisme

- Rédaction de la décision d'homologation

CentraleSupélec

3. Évaluation

d. Bonus RGPD

- À l'aide du logiciel PIA v2.3.0, réaliser l'analyse d'impact sur la protection des données
  - A la fin de la rédaction du PIA penser à l'exporter
  - Le rôle de DPD est tenu par le CSO

Pour aller plus loin

- ANSSI
  - https://www.ssi.gouv.fr/
- Guides de bonnes pratiques
  - https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/
- CNIL
  - https://www.cnil.fr/
- Cyber Malveillance
  - https://www.cybermalveillance.gouv.fr/
- ENISA – European Union Agency for Cybersecurity
  - https://www.enisa.europa.eu/

CentraleSupélec

Merci pour votre attention