SERVICE NUMÉRIQUE DE SANTÉ

PARTENAIRE DIGITAL
AU SERVICE DE LA SANTÉ
DES FRANCILIENS

Gestion des risques liés à la sécurité de l'information

Méthodologie et cas médico-social

Rémi TILLY
Responsable de la Sécurité des Systèmes d'Information
SESAN

SESAN est une marque du GCS D-SISIF

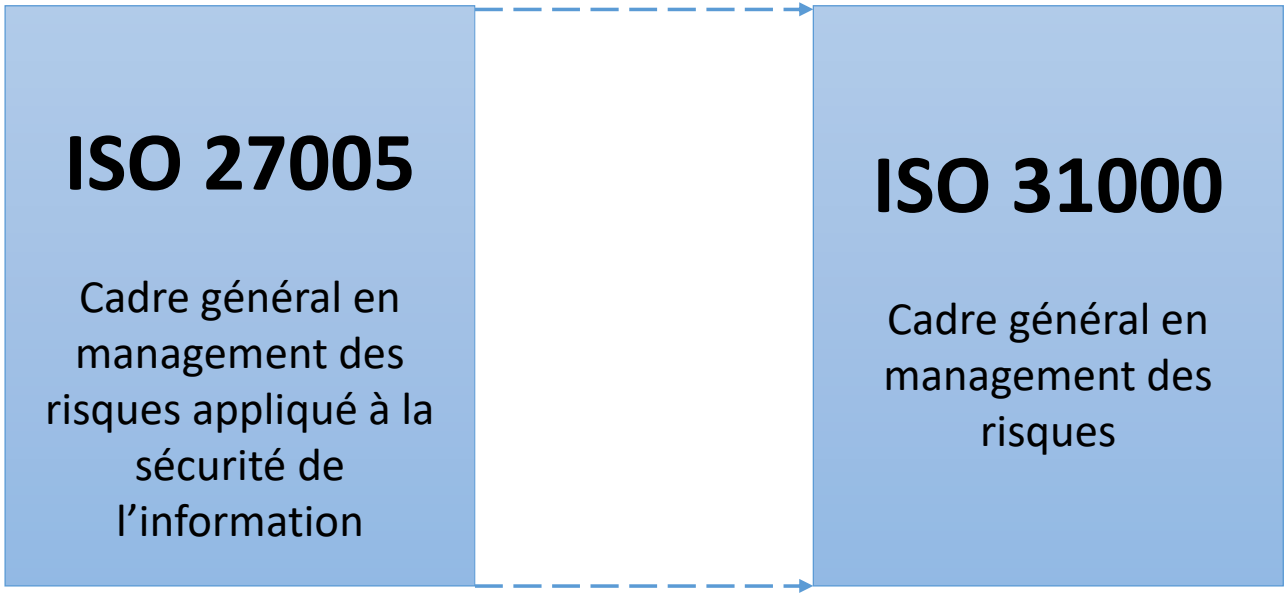
15 juin 2018

SOMMAIRE

Introduction

Normes ISO

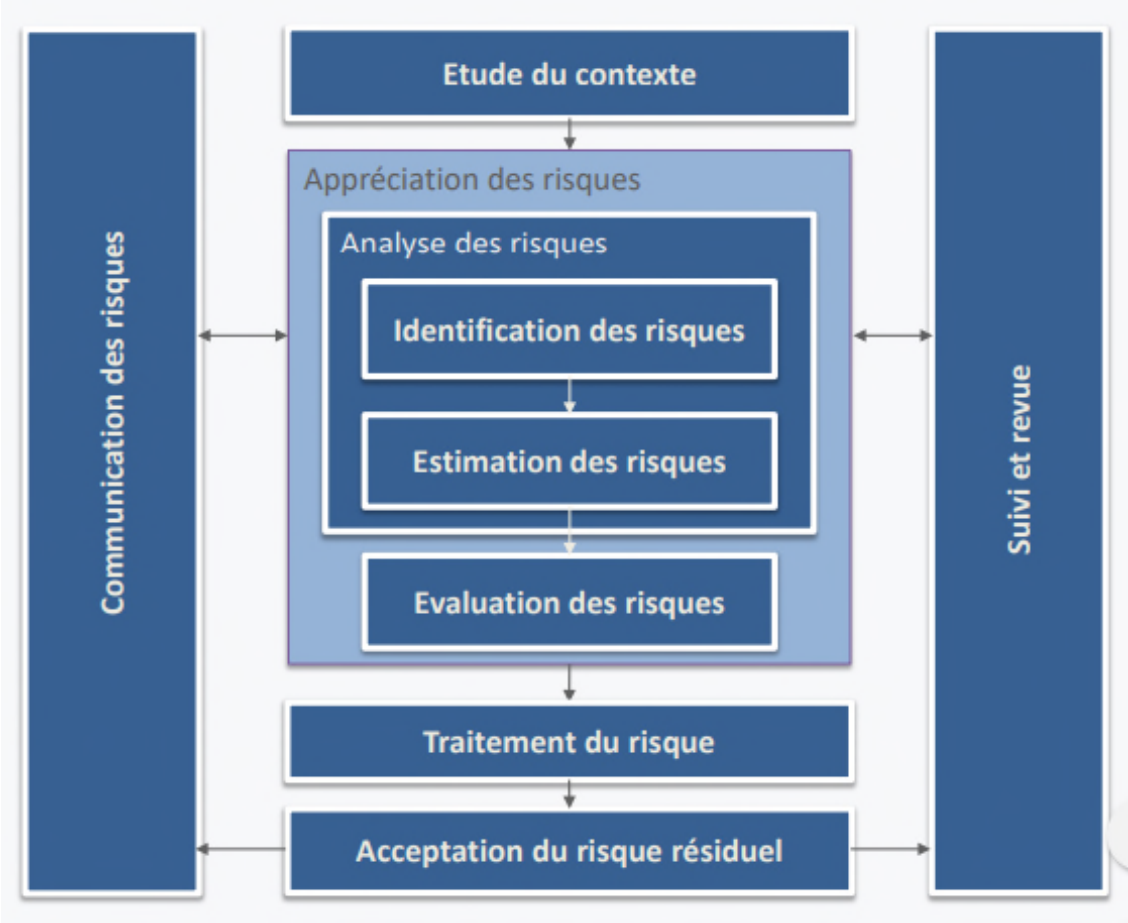
- Adaptation du cadre de référence de l'ISO 31000 pour la sécurité de l'information



Selon la structure de ISO 31000, la norme ISO 27005 explique en détail comment conduire l'appréciation et le traitement du risque dans le cadre de la sécurité de l'information

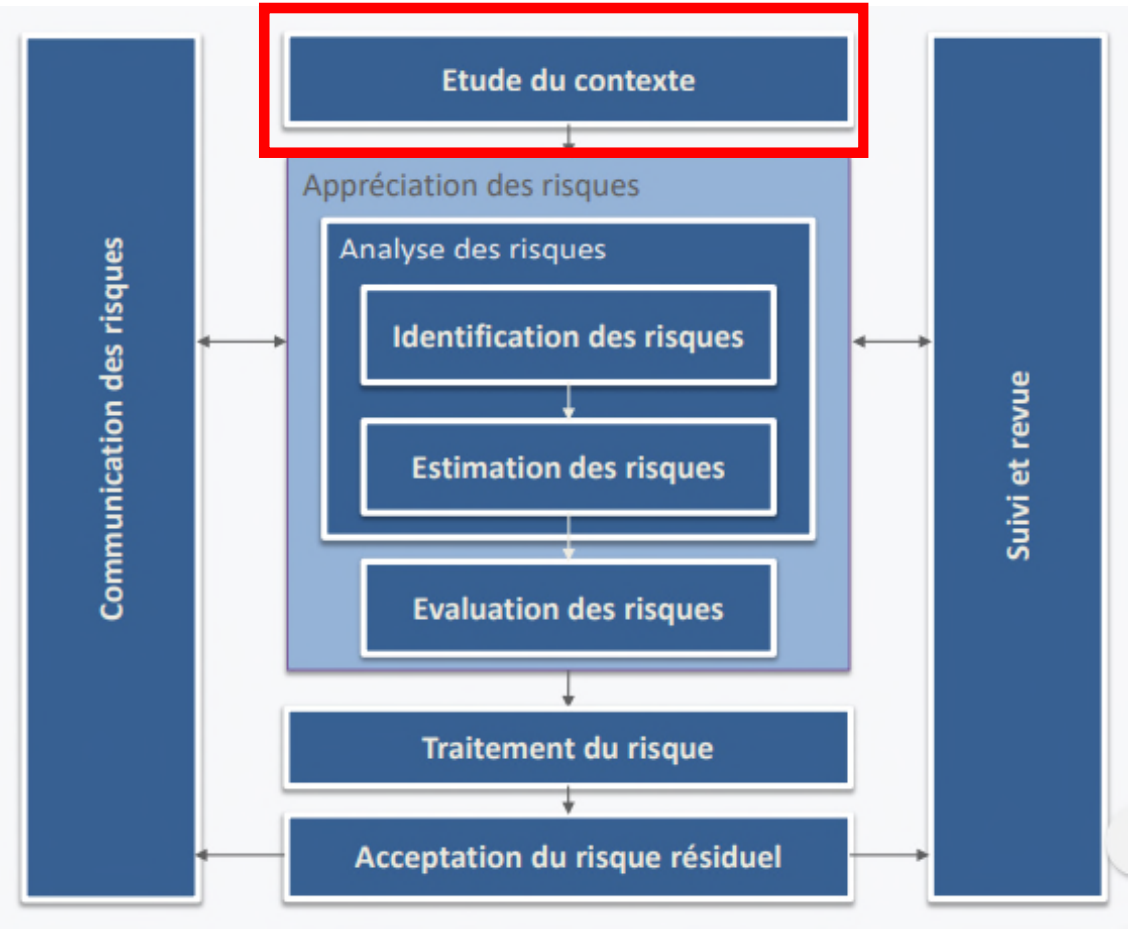
Introduction

Processus de gestion du risque de la sécurité de l'information



Méthodologie et cas médico-social

Etude du contexte



Méthodologie et cas médico-social

Etude du contexte

Identifier / faire évoluer le périmètre

- Processus métier
- Localisations
- Exigences légales
- …

Définition des critères de base

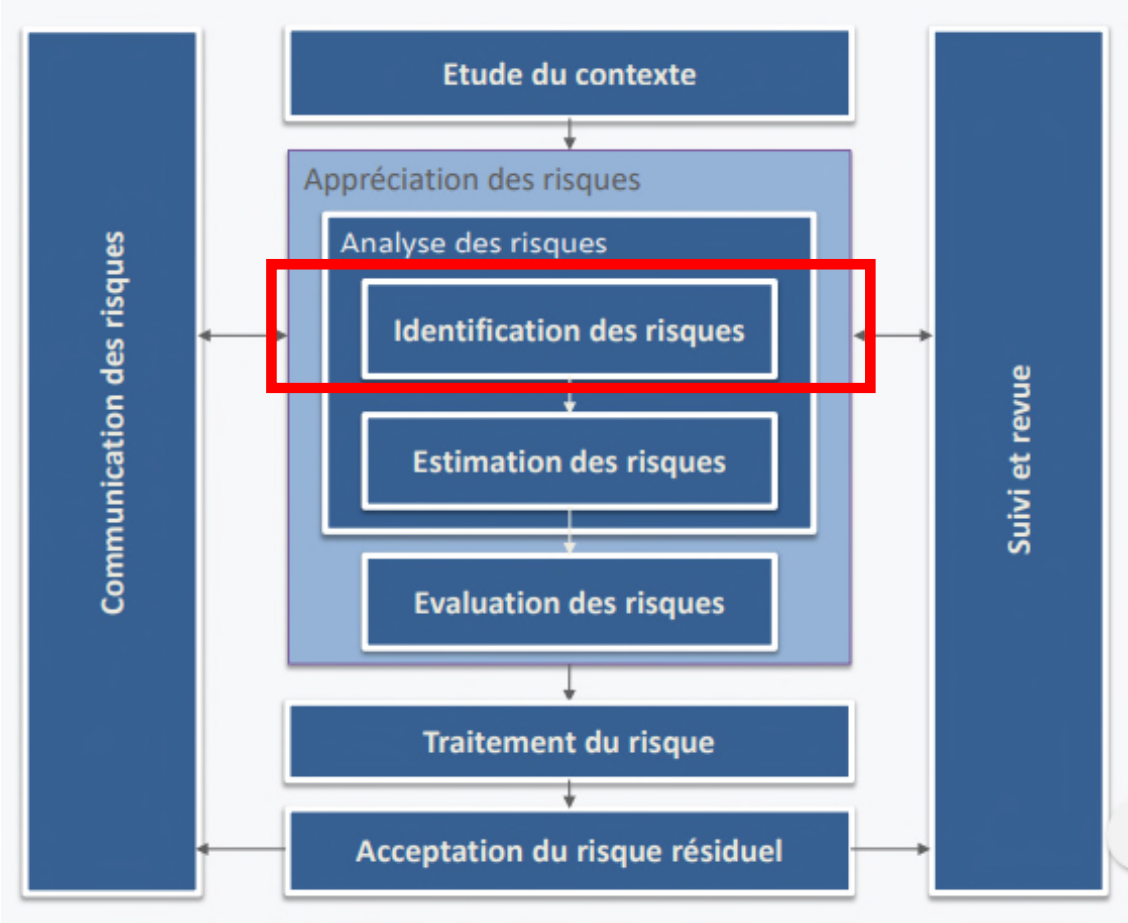
- Valorisation des actifs
- Impact
- Vraisemblance
- Evaluation des risques
- Acceptation des risques

Définir l'organisation

- Rôles et responsabilités
- Processus d'escalade
- Eléments de preuve à conserver

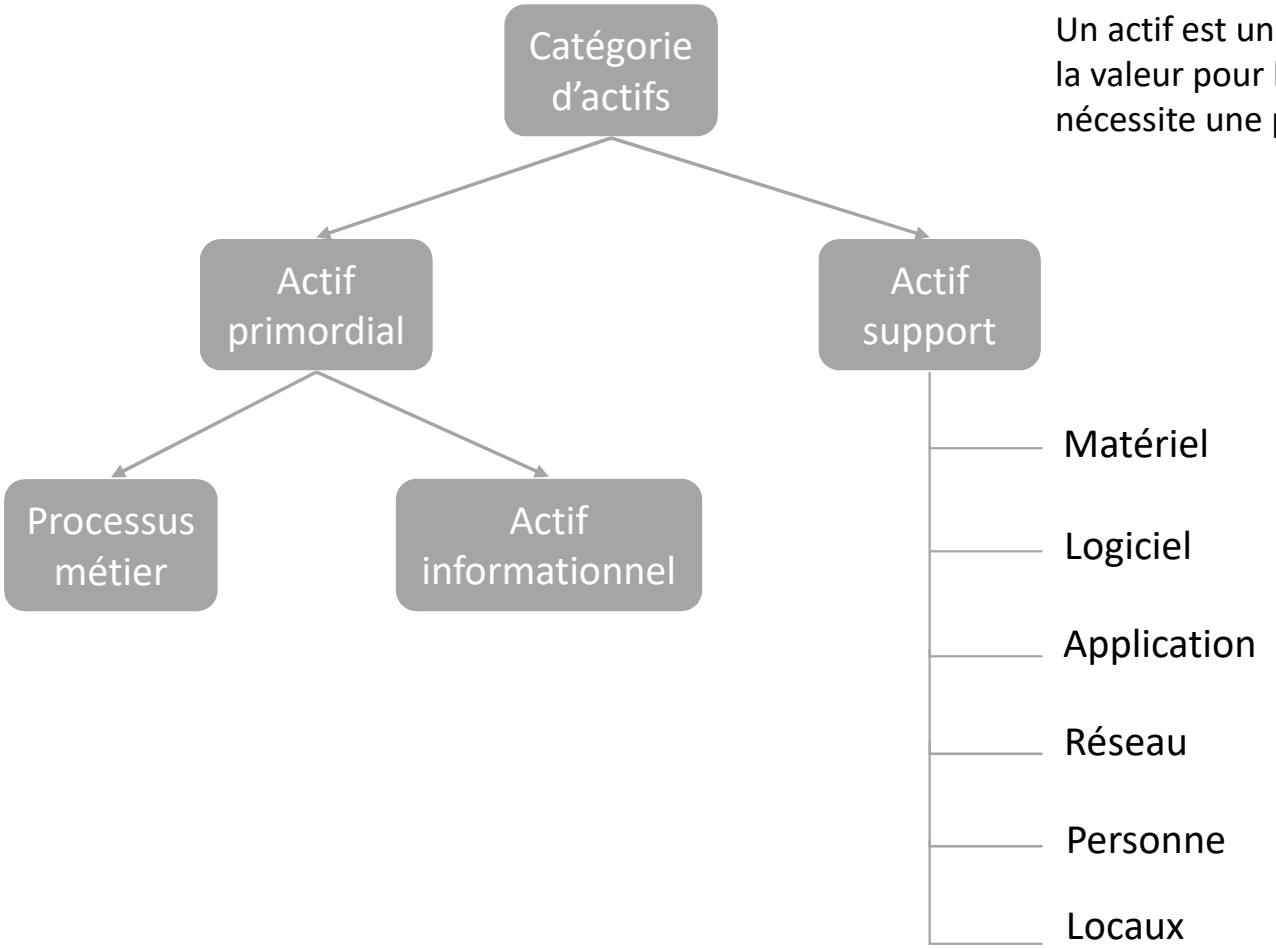
Méthodologie et cas médico-social

Identification du risque



IDENTIFICATION DU RISQUE

Inventaire des actifs



Un actif est un élément représentant de la valeur pour l'établissement et nécessite une protection

IDENTIFICATION DU RISQUE

Inventaire des actifs

Actif primordial

- Activités de l'établissement
- Processus métiers et leurs informations

Actif support

- Support de l'information : logiciel, fichier, équipement, document…

IDENTIFICATION DU RISQUE

Inventaire des actifs primordiaux

Pour identifier les actifs primordiaux, la cartographie fonctionnelle de l'établissement peut aider.

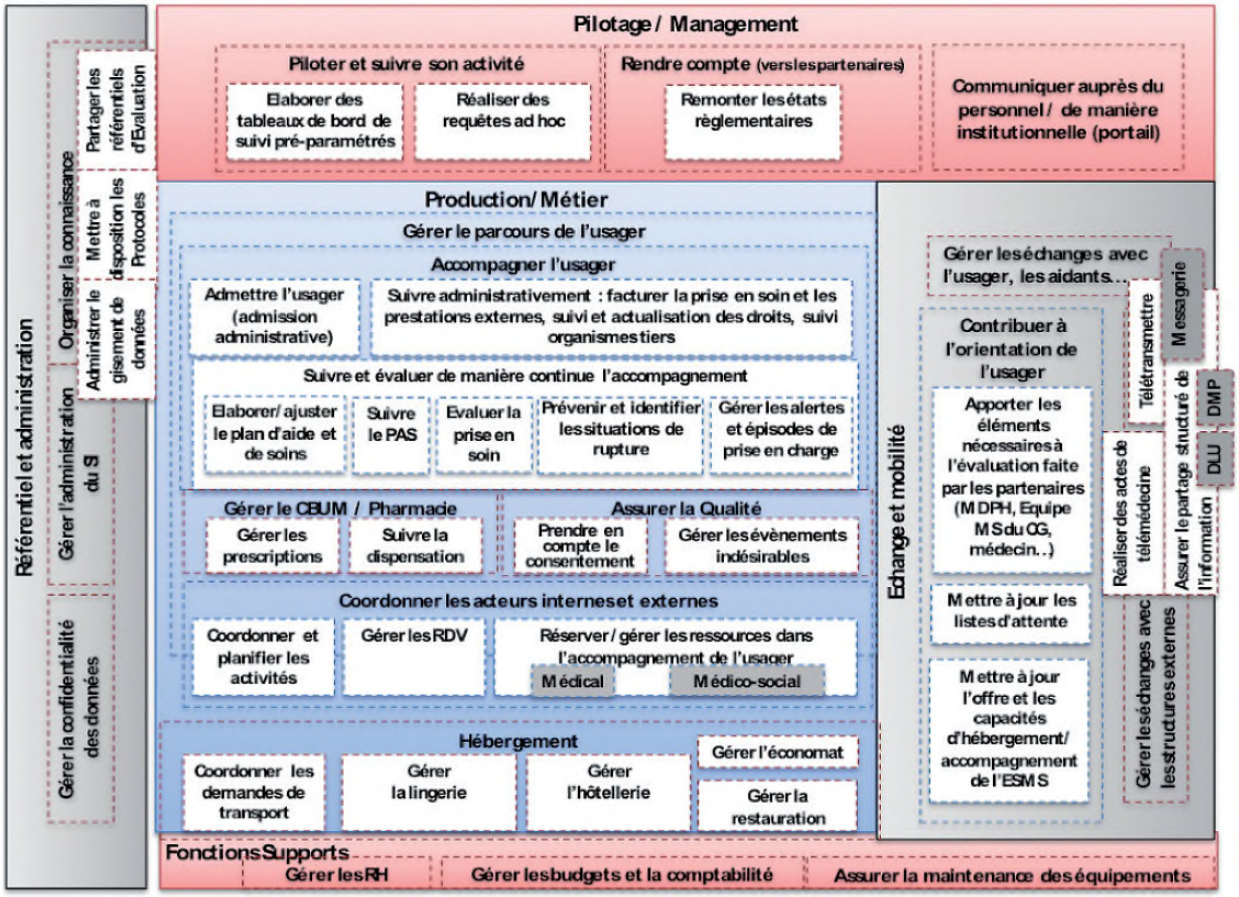


Schéma extrait du guide «Systèmes d'information dans le secteur médico-social » de l'ANAP

IDENTIFICATION DU RISQUE

Cas médico-social : Inventaire des actifs primordiaux

Actifs primordiaux

- Processus :
  - Gestion de la facturation
  - Gestion de la comptabilité et des finances
  - Gestion des ressources humaines
  - Processus logistiques
  - Management stratégique et Gouvernance
  - Gestion des systèmes d'information

- Actifs informationnels :
  - Dossier usager et dossier de soins pour les EHPAD
  - Dossier usager et dossier de soins pour les aides sociales à l'enfance et handicap

IDENTIFICATION DU RISQUE

Cas Médico-Social : Inventaire des actifs supports

Actifs supports

- Matériels :
  - Serveurs
  - Postes de travail
  - Imprimantes et scanners
  - Téléphones mobiles et fixes
- Locaux :
  - Salles serveurs
- Logiciels :
  - Citrix
  - Active Directory
  - Messagerie
- Réseaux :
  - Communication externe
  - Equipements actifs interne
- Personnes :
  - Personnel administratif
  - Personnel éducatif
  - Personnel médical
- Applications :
  - Système Comptabilité et Finances
  - Système Facturation
  - Système des Ressources Humaines
  - Serveurs de résultats
  - Gestion Administrative de l'Usager
  - Dossier de soin
  - Dossier usager
- Prestataires
  - HADS
  - Editeurs

IDENTIFICATION DU RISQUE

Qualification des actifs

- Qualifier le besoin métier en sécurité selon les critères de sécurité : D (Disponibilité) I (Intégrité) C (Confidentialité) et T (Traçabilité) selon l'échelle suivante :

Niveau du besoin		Qualification du besoin métier en			
		Disponibilité	Intégrité	Confidentialité	Traçabilité
1	**Faible**	DMIA < 36h par mois ou de 18j par an	Perte de données sans conséquence	Public	Pas d'exigence
2	**Significatif**	DMIA < 7h par mois ou de 3,5j par an	Conséquence limitée (image de marque…)	Restreint	Des logs existent
3	**Fort**	DMIA < 3h30 par mois ou de 2j par an	Conséquence dommageable (sanctions administratives ou financières)	Restreint contrôlé	Des logs existent et sont protégés
4	**Majeur**	DMIA < 40 min par mois ou de 8h30 par an	Conséquences graves	Secret Médical	Preuve opposable

DMIA : Durée Maximale d'Interruption Maximale

IDENTIFICATION DU RISQUE

Cas Médico-social : Qualification des actifs

Actifs Primordiaux	Impact			
Critères de sécurité	D	I	C	T
Dossier usager et dossier de soins – Aide sociale à l'Enfance et Handicap	3	4	4	4
Dossier usager et dossier de soins - EHPAD	4	4	4	4
Gestion de la comptabilité et des finances	3	4	3	4
Gestion de la facturation	3	4	3	4
Gestion du système d'information	3	3	3	3
Gestion ressources humaines	3	4	3	4
Management stratégique, gouvernance et pilotage	1	3	3	2
Processus logistiques	2	3	2	2

Ici, selon les besoins métiers, les données du dossier usager et du dossier de soins :

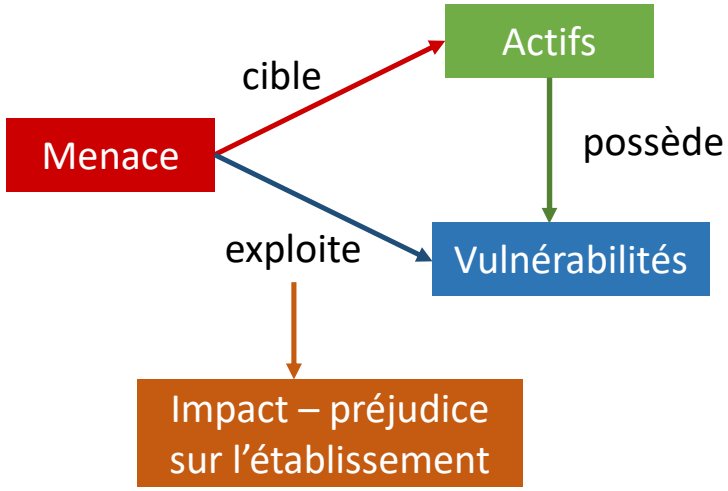
- doivent être disponibles 24/7 avec une durée maximale d'interruption admissible de 40 min par mois (D)
- doivent être intègres (I)
- doivent être du secret médical (C)
- doivent bénéficier d'un haut niveau de traçabilité (T)

L'actif est qualifié par les métiers.

IDENTIFICATION DU RISQUE

Identification des vulnérabilités et des menaces

- Pour chaque actif sélectionné, il faut identifier :
  - Les menaces
  - Les vulnérabilités
  - Les mesures de sécurité existantes
  - Les scénarios de risque
  - La vraisemblance et la gravité du risque



Une menace est la cause potentielle de nuire des actifs tels que des informations, des processus et des systèmes

Une vulnérabilité est une propriété d'un actif qui peut être exploitée par une menace

La vraisemblance est la probabilité qu'un évènement se produise

La gravité mesure la gravité des conséquences attendues en cas de survenance du risque

- Ex : Un virus affecte la Messagerie par Absence d'un antivirus et porte atteinte à la Disponibilité, Intégrité et Confidentialité

IDENTIFICATION DU RISQUE

Echelle de vraisemblance et gravité

Echelle de la vraisemblance

Niveau	Libellé	Description
1	**Exceptionnel**	Théoriquement possible, pas de cas rencontré par ailleurs, ou réalisable dans des conditions particulières, très difficiles à obtenir, nécessitant des moyens et compétences très importants. Evènement très rare s'il s'agit d'un accident **(une occurrence sur une période de plusieurs dizaines d'années**).
2	**Peu probable**	Cas déjà rencontré une ou plusieurs fois, rarement **(une occurrence sur une période d'une dizaine d'années)** pour un incident d'origine involontaire, ou réalisable dans des conditions difficiles pour une malveillance, avec nécessité de personnes organisées, très compétentes et disposant de moyens importants, ou malveillance présentant peu d'intérêt pour son auteur.
3	**Plausible**	Cas rencontré assez fréquemment **(une occurrence sur une période d'une à plusieurs années)** par ailleurs, pouvant se produire avec probabilité pour un incident d'origine involontaire, ou réalisable dans des conditions occasionnelles pour une malveillance, par des personnes ou organisations dotées de moyens limités.
4	**Quasi certain**	Cas auquel le système est de toute façon confronté, fréquent **(plusieurs fois par an),** s'il s'agit d'un incident d'origine principalement involontaire ou réalisable facilement et avec un intérêt évident s'il s'agit d'une malveillance.

IDENTIFICATION DU RISQUE

Echelle de la gravité issue de la PGSSI-S (ASIP-Santé)

Valeur	Patient/Usager	Social & organisation	Financier	Responsabilité / juridique	Réputation / image
1 – Mineure	Gêne / inconfort pour un patient	Gêne ponctuelle dans la prise en charge d'usagers, ou l'activité Démotivation des acteurs / perte de temps	Perte financière sans impact significatif pour le responsable du traitement	Absence de plainte ou plaintes sans suite	Evènement peu ou pas médiatisé, sans effet ou effet négligeable sur l'image de l'organisme.
2 – Significative	Perte de chance pour un patient Effet indésirable limité et réversible sur un patient	Surcharge de travail et/ou désorganisation modérée mais temporaire dans la prise en charge des usagers Conflit social Interruption ou dégradation temporaire de certaines activités	Perte financière avec des impacts modérés pour le responsable du traitement	Contentieux	Dégradation passagère d'image ou de confiance dans l'acteur de santé ou le service offert
3 – importante	Perte de chance pour une population Soins inadéquats et/ou report de soins pour un patient entraînant une mise en danger immédiate du patient (atteinte sévère) et/ou une prolongation de la durée d'hospitalisation et/ou une ré intervention avec ou sans perte de chances	Désorganisation importante et durable de l'activité entraînant une perte significative d'activité et/ou une replanification des soins ou un recours à des organismes tiers. Conflit social paralysant la structure	Perte financière avec des impacts importants pour le responsable du traitement	Atteinte à la vie privée d'un usager Condamnation pénale et/ou financière.	Perte d'image ou de confiance dans l'acteur de santé ou le service offert Mise en cause de la stratégie de l'organisme détenteur du système ou d'un organisme tiers
4 – Critique	Mise en danger d'une population / Menace du pronostic vital Atteinte irréversible ou décès d'un ou plusieurs patient(s).	Arrêt prolongé d'une part importante ou de toute l'activité. Arrêt du projet Fermeture de la structure	Perte financière mettant en cause la pérennité du responsable du traitement	Condamnation pénale et/ou financière Atteinte à la vie privée d'une population Risques judiciaires	Rejet définitif de l'acteur de santé ou du service offert Mise en cause de l'existence de l'organisme détenteur du système ou d'un organisme tiers

IDENTIFICATION DU RISQUE

Cas Médico-Social

Scénario de risque	Vraisemblance	Gravité	Mesures de sécurité mises en œuvre à ce jour
Infection d'un virus sur un poste de travail	4	3	- Antivirus sur les postes de travail - Plan de sauvegarde
Suppression involontaire ou volontaire de données RH	4	3	- Accompagnement au changement - Documentation et formation des utilisateurs - Plan de sauvegarde
Coupure électrique au sein de l'établissement	3	3	- Redondance des onduleurs - Documentation modes dégradés
Accès aux données sensibles du dossier usager par un intervenant non habilité	4	4	- Traces applicatives adaptées aux besoins - Sensibilisation du personnel - Processus de gestion des comptes défini
Fuite d'information confidentielle *(Description : vol perte d'un équipement nomade téléphone, PC Portable, clé USB diffusion sensible)*	3	4	- Sensibilisation du personnel sur les données stratégiques de l'établissement
Accès physique d'une personne non autorisée dans les salles serveurs	1	3	- Liste validée des personnes à accéder dans la salle - Revue des accès physique - Existence d'un processus de gestion des clés

IDENTIFICATION DU RISQUE

Cas Médico-Social

- Focus sur les vulnérabilités et les mesures du scénario « Infection virale sur un poste de travail »

Absence de filtrage web

Filtrage des réseaux

Absence de sensibilisation des utilisateurs

7.2.2 - HN P3.2 - Sensibilisation, apprentissage et formation à la sécurité de l'information des utilisateurs

Absence de gestion des supports amovibles au sein du SI

8.3.1 Gestion des supports amovibles

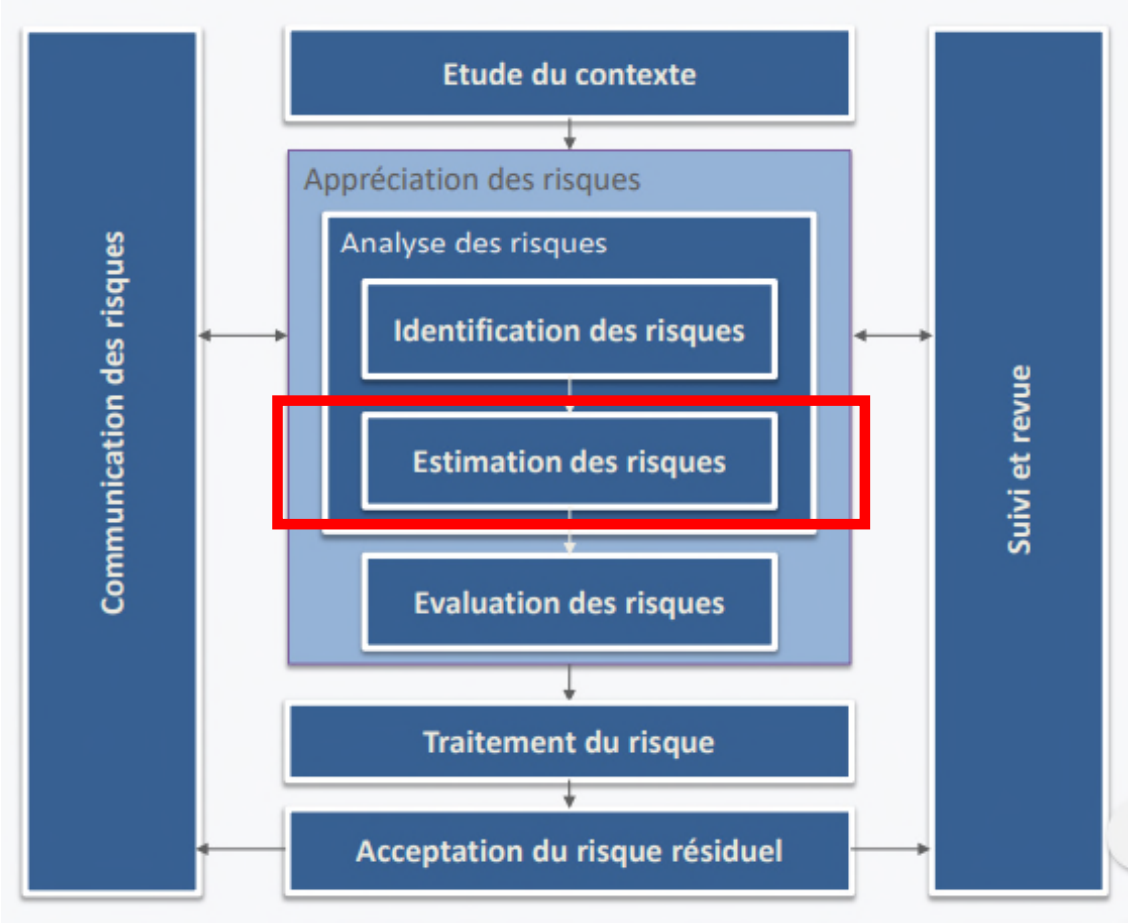
Absence ou défaillance de mécanismes antiviraux (pas d AV, pas de mise à jour, pas de reboot, ...) sur les postes de tra...

12.2.1 Mesures contre les logiciels malveillants (existence, mise à jour)

Mauvaise gestion des comptes d administration (systèmes ou applicatifs) (partage d authentifiant, mot de passe faible...

9.2.3 Gestion des privilèges d'accès (droits restreints au besoin)

ESTIMATION DU RISQUE



ESTIMATION DU RISQUE

- Pour chaque scénario de risque, il faut :
  - Associer les actifs liés au scénario
  - Indiquer l'impact en DICT
  - Indiquer la gravité et la vraisemblance
  - Calculer le niveau de risque brut
    - ❑ Niveau de risque Brut = Max(DICT) x Vraisemblance x Gravité

ESTIMATION DU RISQUE

Cas Médico-Social

Scénario de risque	Actifs primordiaux	D	I	C	T	Vraisemblance	Gravité	Niveau de risque
Infection d'un virus sur un poste de travail	Tous les actifs primordiaux	4	4	4	4	4	3	48
Altération involontaire ou volontaire de données RH	Gestion des RH	3	4	3	4	4	3	48
Coupure électrique au sein de l'établissement	Tous les actifs primordiaux	4	4	4	4	3	3	36
Accès aux données sensibles du dossier usager par un intervenant non habilité	Dossier usager	4	4	4	4	4	4	64
Fuite d'information confidentielle	Management stratégique, gouvernance	1	3	3	2	3	4	36
Accès physique d'une personne non autorisée dans les salles serveurs	Tous les actifs primordiaux	4	4	4	4	1	3	12

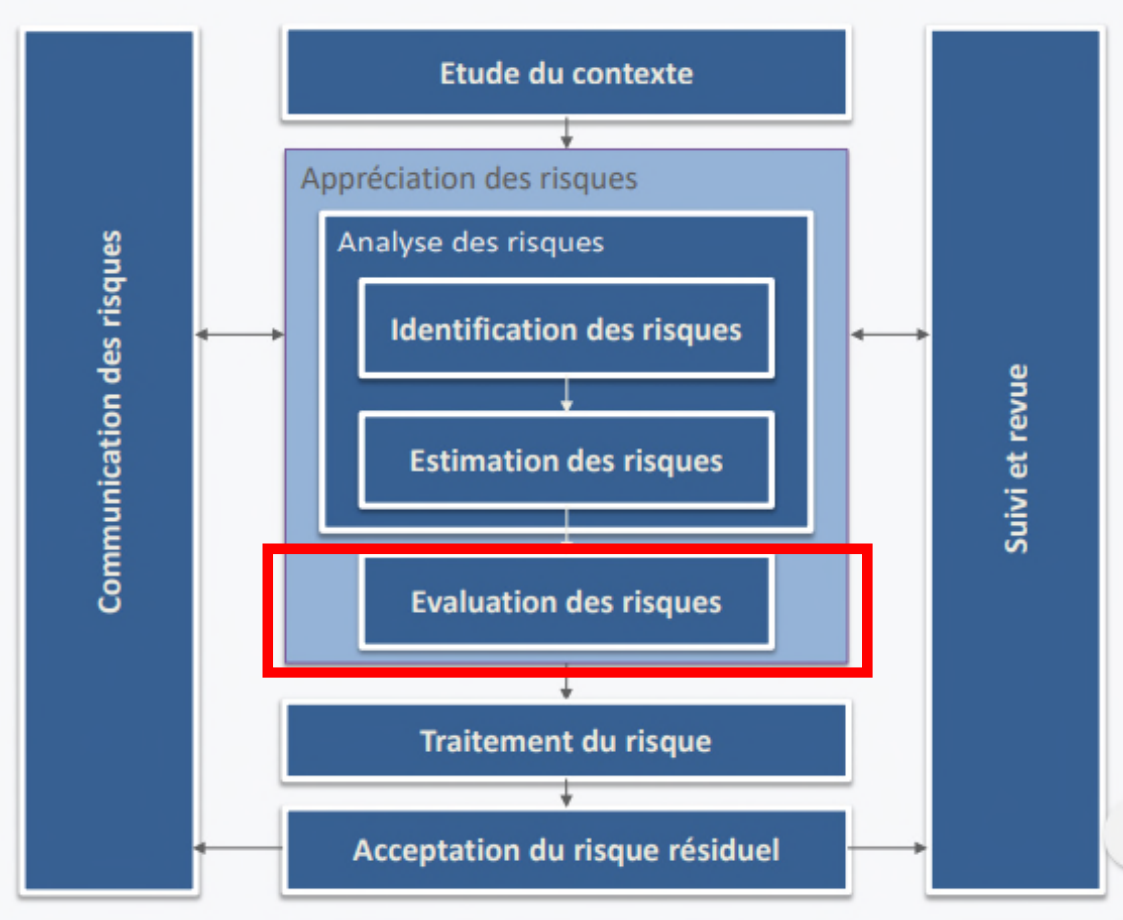
Niveau de risque = Max(DICT) x Vraisemblance x Gravité

ESTIMATION DU RISQUE

Cas Médico-Social

Scénario de risque	Mesures de sécurité mises en œuvre à ce jour	Niveau de risque
Infection d'un virus sur un poste de travail	- Antivirus sur les postes de travail (vrais.) - Plan de sauvegarde (grav.)	48
Suppression involontaire ou volontaire de données RH	- Accompagnement au changement (vrais.) - Documentation et formation des utilisateurs (vrais.) - Plan de sauvegarde (grav.)	48
Coupure électrique au sein de l'établissement	- Redondance des onduleurs (vrais.) - Documentation modes dégradés (grav.)	36
Accès aux données sensibles du dossier usager par un intervenant non habilité	- Traces applicatives adaptées aux besoins (grav.) - Sensibilisation du personnel (vrais.) - Processus de gestion des comptes défini (vrais.)	64
Fuite d'information confidentielle *(Description : vol perte d'un équipement nomade téléphone, PC Portable, clé USB diffusion sensible)*	- Sensibilisation du personnel sur les données stratégiques de l'établissement (vrais.)	36
Accès physique d'une personne non autorisée dans les salles serveurs	- Liste des personnes autorisées à accéder dans la salle (vrais.) - Revue des accès physiques (vrais.) - Existence d'un processus de gestion des clés (vrais.)	12

EVALUATION DU RISQUE



EVALUATION DU RISQUE

Cas Médico-Social

Matrice d'évaluation

Gravité / vraisemblance	Exceptionnel (1)	Peu probable (2)	Plausible (3)	Quasi certain (4)
Critique (4)	2	2	3	3 A
Important (3)	1 F	2	2 D	3 B C
Significatif (2)	1	2	2	2 E
Mineur (1)	1	1	1	1

Echelle du niveau de risque :

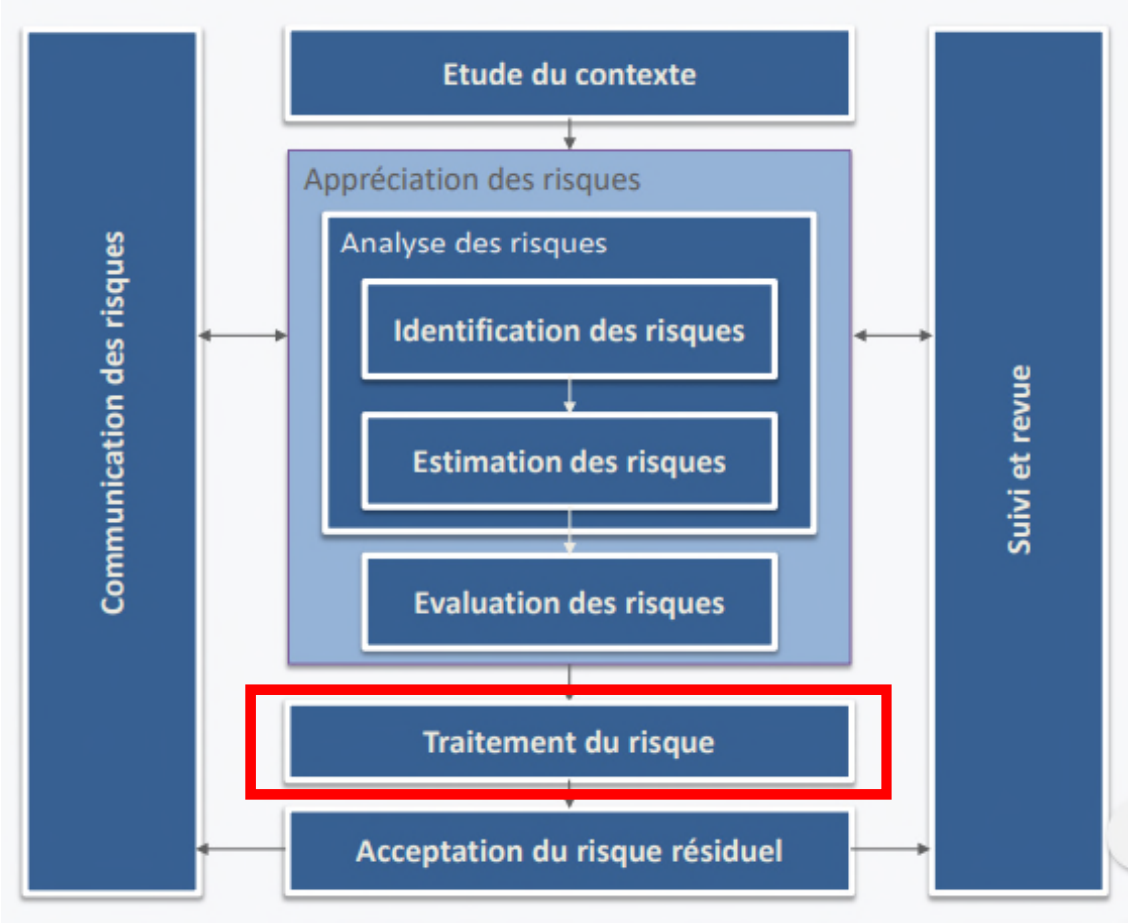
Niveau de risque Fort de 43 à 64 équivaut à 3

Niveau de risque Modéré de 22 à 42 équivaut à 2

Niveau de risque Limité de 1 à 21 équivalent à 1

Réf.	Scénario de risques	Niveau de risque
A	Accès aux données sensibles du dossier usager par un intervenant non habilité	64
B	Infection d'un virus sur un poste de travail	48
C	Altération involontaire ou volontaire des données RH	48
D	Coupure électrique au sein de l'établissement	36
E	Fuite d'information confidentielle	36
F	Accès physique d'une personne non autorisée dans les salles serveurs	12

TRAITEMENT DU RISQUE



TRAITEMENT DU RISQUE

Ce que propose la Direction des Systèmes d'information :

- **Réduire :** La différentes mesures sont proposées pour réduite le risque à un niveau acceptable.
- **Maintenir :** Le niveau est jugé acceptable. décide d'accepter le niveau actuel du risque
- **Eviter :** Le risque est évité, ce qui revient à annuler ou modifier un ensemble d'activités lié au risque
- **Partager :** Le risque est partagé. certains risques avec des parties externes (assurance ou infogérance ou sous-traitance)

TRAITEMENT DU RISQUE

Cas Médico-Social

Scénario de risques	Niveau de risque	Proposition DSI
Accès aux données sensibles du dossier usager par un intervenant non habilité	64	Réduire
Infection d'un virus sur un poste de travail	48	Réduire
Altération involontaire ou volontaire des données RH	48	Réduire
Coupure électrique au sein de l'établissement	36	Réduire
Fuite d'information confidentielle	36	Réduire
Accès physique d'une personne non autorisée dans les salles serveurs	12	Maintenir

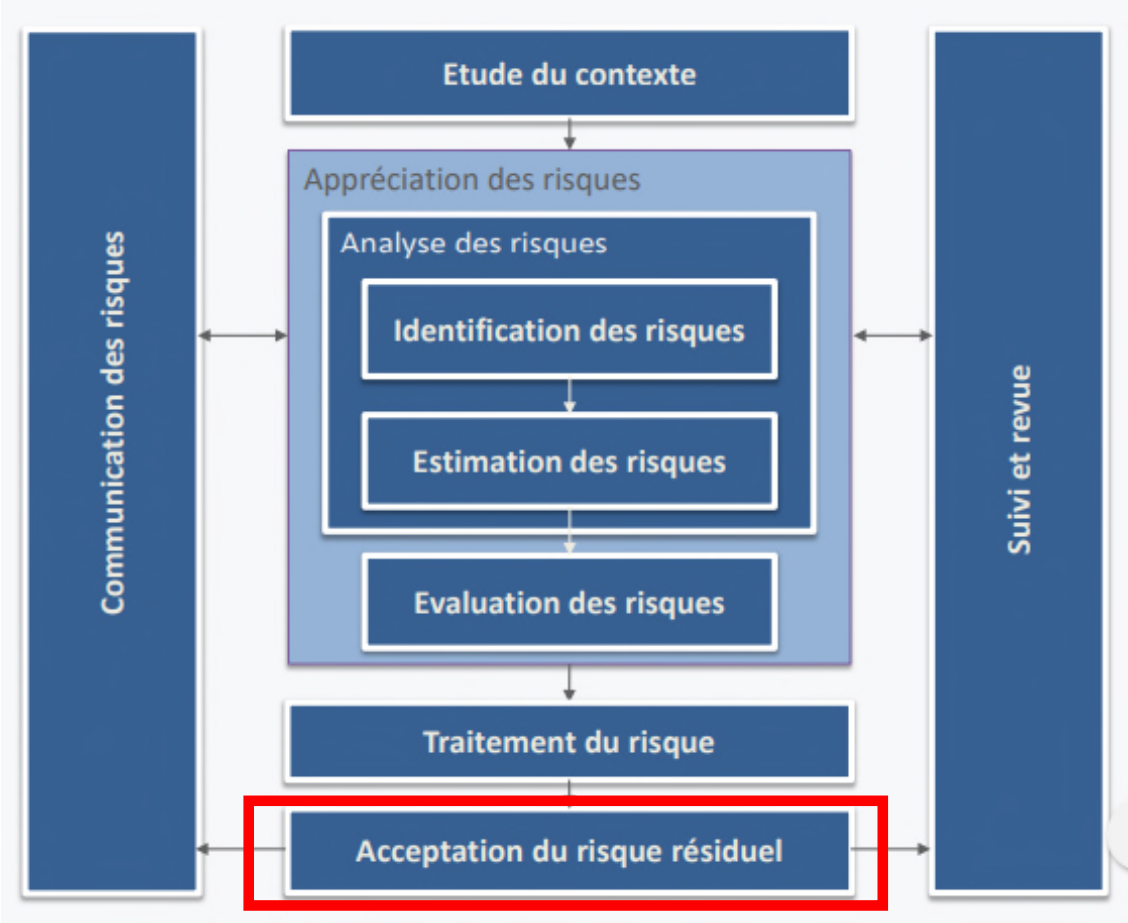
TRAITEMENT DU RISQUE

Cas Médico-Social

Scénario de risque	Niveau de risque	Décision DSI	Mesures programmées
Accès aux données sensibles du dossier usager par un intervenant non habilité	64	Réduire	- Renforcement de la politique des mots de passe - Sensibilisation du personnel
Infection d'un virus sur un poste de travail	48	Réduire	- Contrôle des droits d'administration sur les postes - Blocage des ports USB sur les postes de travail - Sensibilisation du personnel
Altération involontaire ou volontaire des données RH	48	Réduire	- Contrôle sur les informations sensibles renseignées - Tests de restauration - Sensibilisation du personnel
Coupure électrique au sein de l'établissement	36	Réduire	- Tests des dispositifs de secours - Dispositif de supervision de l'alimentation électrique
Fuite d'information confidentielle	36	Réduire	- Revue des comptes utilisateurs - Profils applicatifs adaptés à la fonction de l'agent - Sensibilisation du personnel
Accès physique d'une personne non autorisée dans les salles serveurs	12	Maintenir	

Une seule mesure peut réduire le niveau de risque de plusieurs scénarii.

ACCEPTATION DU RISQUE RESIDUEL



ACCEPTATION DU RISQUE RESIDUEL

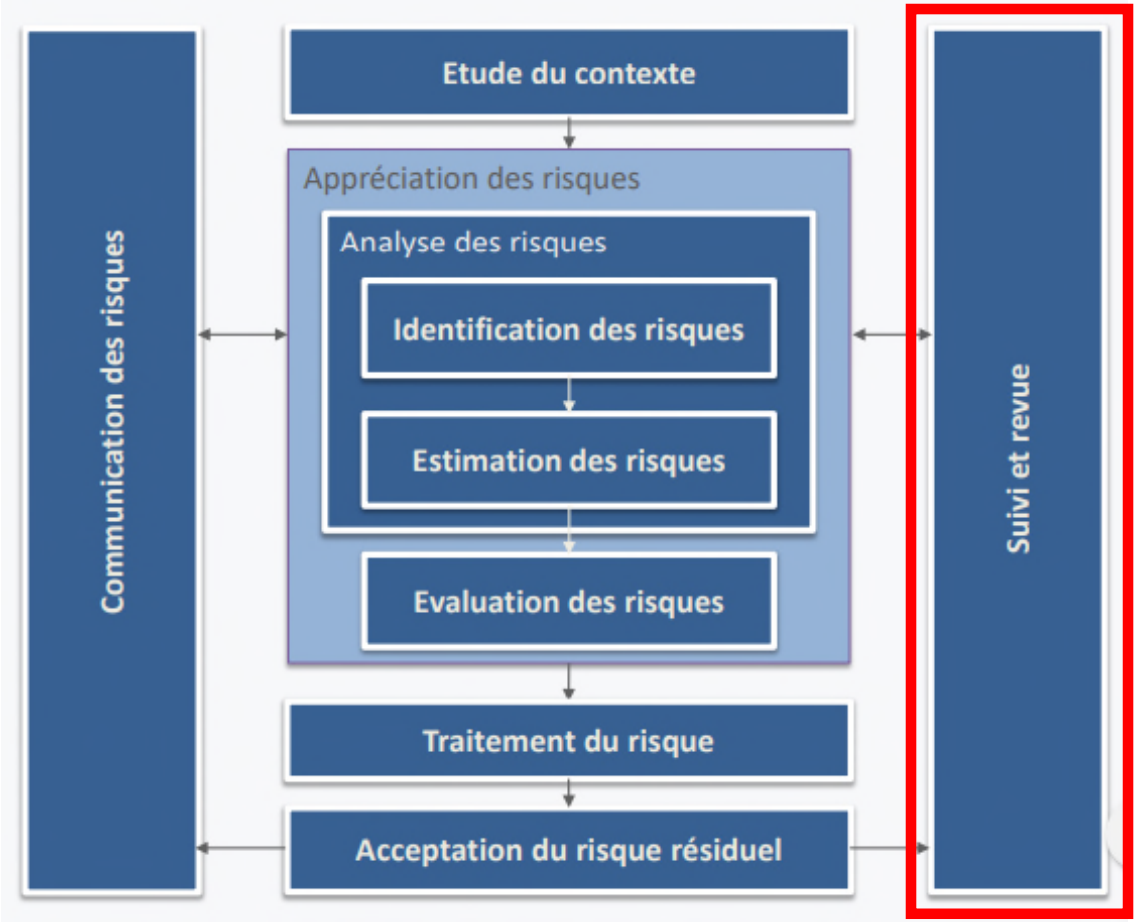
Ce que décide la Direction Générale

- Accepter/Refuser les mesures de sécurité proposées par la DSI
- Accepter/Refuser le niveau résiduel

Le but de l'acceptation est de s'assurer de la cohérence du plan de traitement des risques, avant sa mise en œuvre.

La validation permet une acceptation officielle des mesures proposées et l'établissement du plan d'action.

SUIVI ET REVUE



La gestion des risques est un processus à déployer dans la durée. L'environnement change en permanence faisant évoluer le contexte, les menaces et les vulnérabilités.

Une revue de l'analyse de risques doit être réalisée de préférence à minima 1 fois par an.

QUESTIONS ?

Rémi TILLY
Responsable de la Sécurité des Systèmes d'Information
SESAN
remi.tilly@sesan.fr