La gestion des risques selon la norme ISO27701

Forum Sécurité @Cloud

Keynote

24 sept. 2020

Amélie PAGET
Consultante indépendante - Protection des données personnelles
Formatrice HS2

HS2
Hervé Schauer Sécurité

La gestion des risques selon la norme ISO27701

1. ISO27701 - Présentation de la norme

2. PIMS – Processus de gestion des risques

© Hervé Schauer Sécurité

Présentation de la norme ISO27701

© Hervé Schauer Sécurité

Norme ISO27701

ISO 27701:2019

Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de a protection de la vie privée – Exigences et lignes directrices

Security techniques – Extension to ISO/IEC 27001and ISO/IEC 27002 for privacy information management – Requirements and guidelines

1ère édition 2019-08

En Anglais et en Français

80 pages (Fr)

© Hervé Schauer Sécurité

Norme ISO27701

Norme Internationale qui permet de :

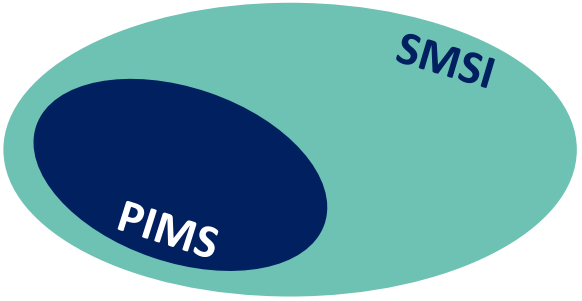
- Intégrer les exigences et bonnes pratiques en matière de vie privée à un **système de management**
  - Processus documenté, pérenne, auditable ; amélioration continue
- Adopter une démarche de **gouvernance** de la protection de la vie privée
- Intégrer les **exigences légales et réglementaires** applicables
  - Pas uniquement le RGPD
- Répondre au principe d'***Accountability***
- **Certifier** un système de management de protection de la vie privée
  - Ou ***PIMS – Privacy Information Management System***

© Hervé Schauer Sécurité

Norme ISO27701

Extension des normes ISO27001 et ISO27002

- Apporte des **spécifications aux exigences de l'ISO27001**
- Ajoute des **recommandations spécifiques et supplémentaires aux mesures de l'ISO27002**
- Implique un **SMSI** sur l'ensemble du périmètre du **PIMS**
  - Mais pas nécessairement un périmètre confondu



S'adresse à tout type d'organisme

- Privé ou public, **Responsable de traitement** (RT) et **Sous-traitant** (ST)

© Hervé Schauer Sécurité

Norme ISO27701

Structure du document

- Respecte le HLS (*High Level Structure*) des normes ISO dédiées aux systèmes de management

  - Avant-propos
  - Introduction
  1. Domaine d'application
  2. Références normatives
  3. Termes, définitions et abréviations
  4. Généralités
  5. **Exigences** spécifiques au PIMS liées à l'ISO27001
  6. **Recommandations spécifiques au PIMS** liées à l'ISO27002
  7. **Recommandations supplémentaires pour les RT**
  8. **Recommandations supplémentaires pour les ST**
  - Annexes

© Hervé Schauer Sécurité

Structure du document

Annexes

Annexe A (normative) : **Objectifs et mesures de référence spécifiques au PIMS (responsables de traitement)**

Annexe B (normative) : **Objectifs et mesures de référence spécifiques au PIMS (sous-traitants)**

Annexe C (informative) : Correspondance avec l'ISO/IEC 29100

Annexe D (informative) : **Correspondance avec le Règlement général sur la protection des données**

Annexe E (informative) : Correspondance avec l'ISO/IEC 27018 et l'ISO/IEC 29151

Annexe F (informative) : **Comment appliquer l'ISO/IEC 27701 à l'ISO/IEC 27001 et l'ISO/IEC 27002**

Bibliographie

© Hervé Schauer Sécurité

Norme ISO27701

Articulation avec les normes ISO27001 et ISO27002

Dans le corps des normes ISO27001 et ISO27002

- Remplacer « sécurité de l'information »
  - par « **sécurité de l'information et protection de la vie privée** »

Article 5	**précise** certaines exigences de l'ISO27001
Article 6	**complète** certaines recommandations de l'ISO27002
Article 7	**ajoute** de nouvelles recommandations à destination des **RT**
Article 8	**ajoute** de nouvelles recommandations à destination des **ST**

© Hervé Schauer Sécurité

Norme ISO27701

Articulation avec les normes ISO27001 et ISO27002

Article 5 **précise** certaines exigences de l'ISO27001 ← Exigences Gouvernance

Article 6 **complète** certaines recommandations de l'ISO27002 ← Recommandations Sécurité des données

Article 7 **ajoute** de nouvelles recommandations à destination des **RT**

Article 8 **ajoute** de nouvelles recommandations à destination des **ST**

← Recommandations Protection de la vie privée

© Hervé Schauer Sécurité

Norme ISO27701

Quid de la norme ISO27018

ISO/IEC 27018:2014

Technologies de l'information — Techniques de sécurité

Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

- Déclinaison des normes :
  - ISO 17788 (cadre et vocabulaire du *Cloud*),
  - ISO 27002 (bonnes pratiques de sécurité de l'information)
  - ISO 29100 (principes de protection de la vie privée).
- Mesures recommandées pour un fournisseur de *cloud computing* hébergeant des DCP pour le compte d'un RT
- Ne traite pas de la gouvernance chez l'hébergeur

© Hervé Schauer Sécurité

Norme ISO27701

Quid de la norme ISO27018

La norme ISO27701 :

- **Reprend le contenu** de la norme ISO27018 à son article 8 consacré aux sous-traitants
- **Met à jour** les dispositions de l'ISO27018
- Est d'application **plus large** que la norme ISO27018

La norme ISO27018 va-t-elle :

- Être absorbée par l'ISO27701 ?
- S'articuler avec l'ISO27701 ?

© Hervé Schauer Sécurité

PIMS - Processus de gestion des risques

© Hervé Schauer Sécurité

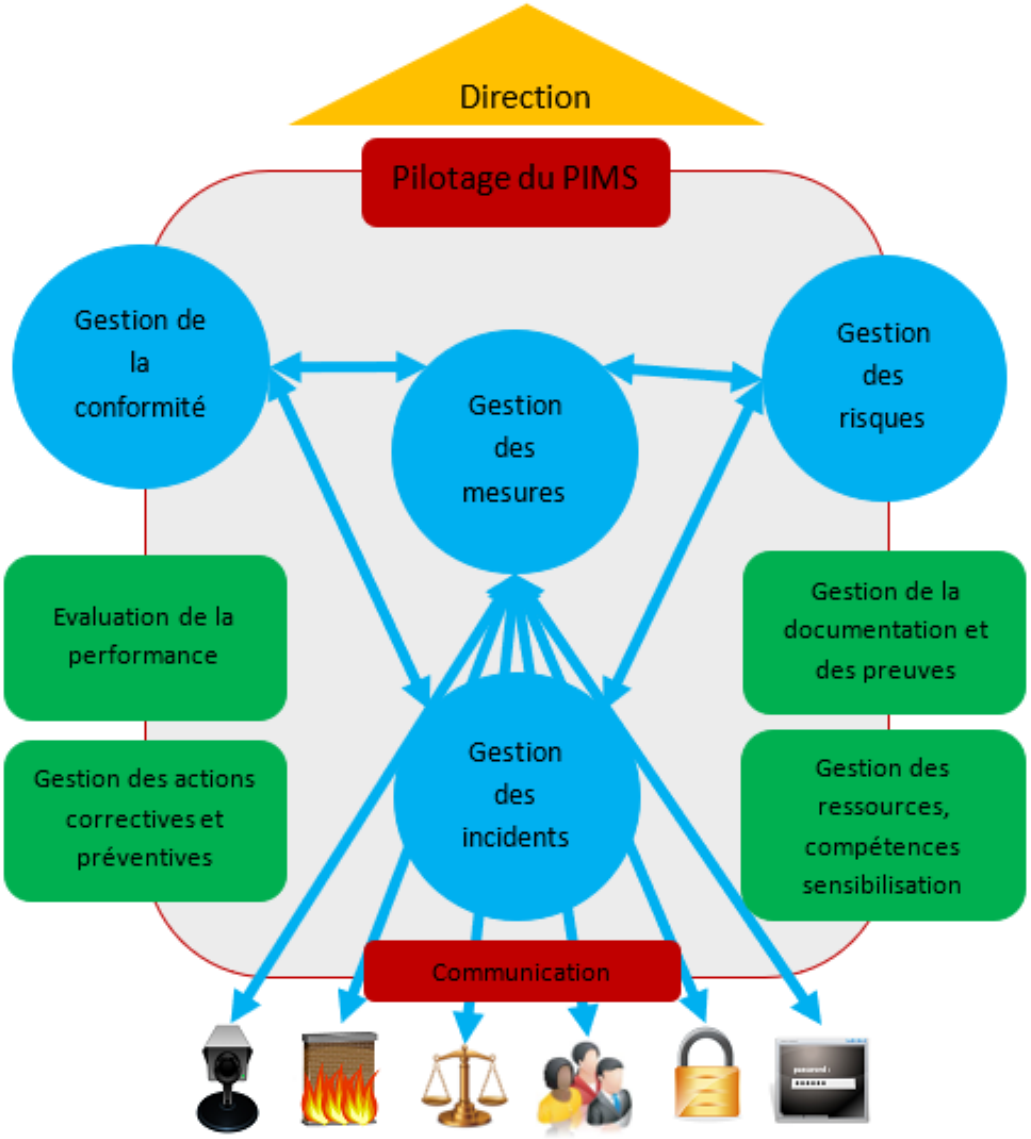
Processus de gestion des risques

Les processus

Pour un PIMS :

- S'appuyer sur les processus existants
- Y intégrer le volet Protection de la vie privée

- Le processus de gestion de la conformité prend du poids

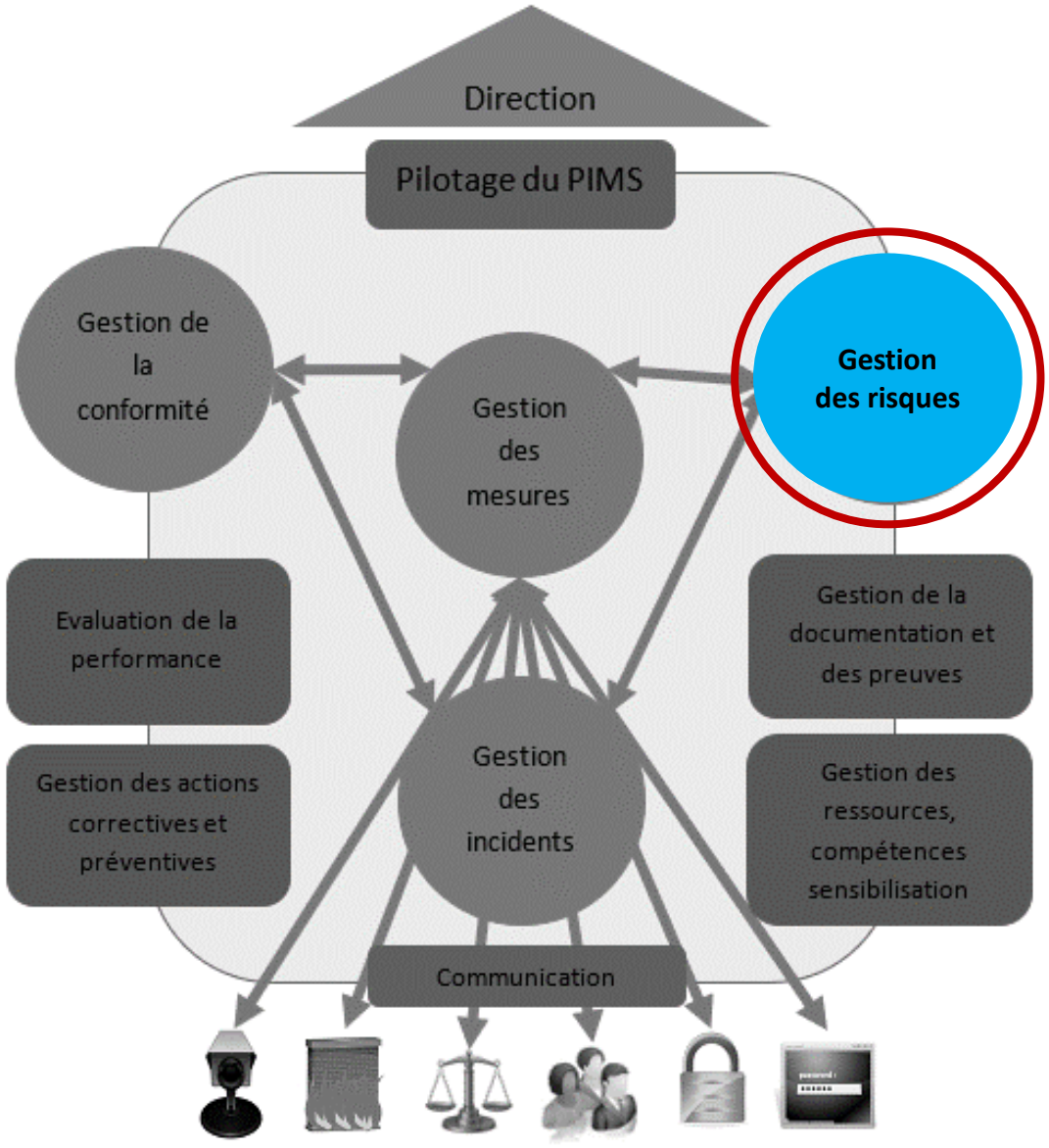


© Hervé Schauer Sécurité

Processus de gestion des risques

Focus

Processus de Gestion des risques



© Hervé Schauer Sécurité

Processus de gestion des risques

Objectifs du processus

- Identifier et apprécier les risques
- Définir un plan de traitement des risques

Eléments d'entrée	Réf.	Activités	Réf.	Eléments de sortie	Réf.
Compréhension de l'organisation et de son contexte	ISO27001 4.1 ISO27701 5.2.1	Appréciation des risques	ISO27001 6.1.2 ISO27701 5.4.1.2	AdR	ISO27001 6.1.2 ISO27701 5.4.1.2
Exigences des parties intéressées	ISO27001 4.2 ISO27701 5.2.2	Traitement des risques	ISO27001 6.1.3 ISO27701 5.4.1.3	DdA et PTR Approbation du PTR Acceptation des risques	ISO27001 6.1.3 ISO27701 5.4.1.3
Domaine d'application	ISO27001 4.3 ISO27701 5.2.3				

Réf. + ISO27005

© Hervé Schauer Sécurité

Processus de gestion des risques

2 volets

Réf. ISO27701 5.4.1.2

1. Appréciation des risques **pour la sécurité de l'information**
2. Appréciation des risques **sur la vie privée**

- Soit 1 processus unique couvrant l'ensemble de ces risques
- Soit 2 processus distincts.

© Hervé Schauer Sécurité

Notion de risque

Réf. ISO27701 5.4.1.2

2 catégories de risques :

1. **Risques de sécurité de l'information** : risques liés à la perte de confidentialité, d'intégrité et de disponibilité entrant dans le périmètre du PIMS,
   - En particulier ceux impactant les DCP et leur traitement
2. **Risques sur la vie privée** : risques liés au traitement des DCP, entrant dans le périmètre du PIMS
   - A quoi cela correspond ?

© Hervé Schauer Sécurité

Risques de sécurité de l'information

Actifs primordiaux :

- Données à caractère personnel (DCP)
- Processus liés aux traitements de DCP

Conséquences potentielles :

- Pour l'organisation
- Pour les personnes concernées (PC)

© Hervé Schauer Sécurité

Conséquences pour les PC

Echelle proposée : (inspirée des outils CNIL)

Niveau	Conséquences sur les personnes concernées
1-Insignifiant	Les PC ne seront pas affectées ou pourraient rencontrer quelques inconvénients mineurs (perte de temps , simple contrariété…)
2-Limité	Les PC pourraient rencontrer des inconvénients qu'elles seraient capables de surmonter sans difficulté (complexification de démarches administratives, frais mineurs, …) Peut avoir conséquences insignifiantes pour un nombre massif de PC
3-Signifiant	Les PC pourraient subir des conséquences significatives qu'elles seraient capables de surmonter mais avec difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, affection physique ou psychologique mineure, etc...) Peut avoir conséquences limitées pour un nombre massif de PC
4-Maximum	Les PC pourraient rencontrer des conséquences significatives, voire irréversibles ou insurmontables (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, affection physique ou psychologique grave…) Peut avoir conséquences signifiantes pour un nombre massif de PC

© Hervé Schauer Sécurité

Processus de gestion des risques

Risques sur la vie privée

Réf. ISO27701 5.4.1.2

- Pas d'impact CID
- Mais des atteintes aux principes fondamentaux de la protection de la vie privée

ISO29134 6.4.4.1

Cela peut notamment inclure :

- Collecte excessive de DCP (perte de maîtrise opérationnelle)
- Corrélation non-autorisée ou inappropriée de DCP
- Informations insuffisantes concernant l'objet du traitement des DCP (manque de transparence)
- Absence de prise en compte des droits de la PC (ex. perte du droit d'accès)
- TDCP à l'insu ou en l'absence de consentement de la PC
- Partage ou réaffectation de DCP avec des tiers sans le consentement de la PC
- Conservation inutilement prolongée des DCP

Autres sources :

- **Norme ISO29100** – *Privacy Framework* ou **RGPD**

© Hervé Schauer Sécurité

Processus de gestion des risques

Risques sur la vie privée

Proposition : Atteintes à la vie privée

1 - Atteinte aux principes fondamentaux de :

- Licéité, loyauté et transparence
- Limitation des finalités
- Minimisation des données
- Exactitude des données
- Limitation des durées de conservation
- Protection de la vie privée en cas de transfert, divulgation ou partage de données
- Protection de la vie privée dans le cadre d'un recours à un prestataire (sous-traitant ou co-responsable de traitement)

2- Atteintes aux droits des personnes concernées

- Informations, Consentement, Accès, Rectification, ...

© Hervé Schauer Sécurité

Risque sur la vie privée

Comment apprécier un risque lié à une non-conformité ?

- Pas d'impact en DIC sur les DCP.
- Mais des **atteintes aux principes fondamentaux**.

- Des **conséquences potentielles** pour l'**organisation**
- Et des **conséquences potentielles** pour les **PC**

- La **vraisemblance** dépend peu de la facilité d'exploitation.
- Eventuellement de la **probabilité d'occurrence**.

© Hervé Schauer Sécurité

Processus de gestion des risques

Risque sur la vie privée

Norme ISO29134 (6.4.4.1 NOTE)

Identification des risques :

> « Ces possibilités de non-application ou d'application incorrecte des droits fondamentaux ne peuvent qu'être vérifiées et améliorées. Il est en effet impossible de ne pas appliquer ces droits fondamentaux. »

(6.4.3, 7.4 et 7.5.5)

Prévoit un volet dédié à l'Analyse de la conformité

Outils PIA CNIL

Le volet « Principes fondamentaux »

- Ne fait pas l'objet d'une appréciation/valorisation
- Description des moyens mis en œuvre pour respecter les principes

© Hervé Schauer Sécurité

Risque sur la vie privée

Comment apprécier un risque lié à une non-conformité ?

1. Je ne valorise pas.
   - Choix binaire : Soit ma pratique est conforme soit elle ne l'ai pas.

1. Je valorise.
   - Notamment en fonction des conséquences pour les droits et libertés des personnes.
   - Permet de prioriser les non-conformités et de faciliter mes choix à venir dans le cadre du Plan de traitement des risques.
     - Exemple :

© Hervé Schauer Sécurité

Processus de gestion des risques

Risques sur la vie privée

Quid du scénario d'incident ?

Rappel : Scénario d'incident

Description d'une menace exploitant une vulnérabilité ou un ensemble de vulnérabilités, lors d'un incident de sécurité de l'information

Relie les éléments suivants :

- Actifs supports, Menace, Vulnérabilités, Impacts en DIC et les Conséquences sur les Actifs primordiaux.

→ S'éloigner de ce concept.

© Hervé Schauer Sécurité

Risques sur la vie privée

Quid du scénario d'incident ?

Proposition

- Mesures de protection de la vie privée existantes
- Atteintes aux principes fondamentaux constatés
- Traitements de DCP impactés
- Référence Légale et Réglementaire
- Non-conformité

Mesures de protection de la vie privée existantes	Mise en ô	Atteintes constatées	TDCP impactés	Réf. LR	NC

© Hervé Schauer Sécurité

Risques sur la vie privée

Plan de traitement

Proposition

- Mesures de protection de la vie privée choisie
- Non-conformité résiduelle
  - Conforme ou Remarque
  - Toute NC Mineure doit faire l'objet d'une validation par la Direction (RT ou ST)
  - Une NC Majeure ne peut être acceptée ni validée
- Acceptation par le propriétaire des non-conformités
- Avis DPO et Validation du RT/ST

NC	Mesures sélectionnées	NC résiduelle	Acceptation	Avis DPO	Validation RT

© Hervé Schauer Sécurité

Déclaration d'applicabilité (DdA)

Réf. ISO27701 5.4.1.3

« L'organisation doit définir et appliquer un processus de traitement des risques pour :

d) produire une DdA contenant :

- Les mesures nécessaires (reprendre l'annexe A ISO27001 et les Annexes A et/ou B ISO27701)
- La justification de leur insertion
- Si les mesures nécessaires sont mises en œuvre ou non ;
- Et la justification de l'exclusion de toute mesure des Annexes précitées

NOTE Cette justification peut inclure les cas où les mesures ne sont pas requises par (ou sont soumises à des exceptions en vertu de) la législation et/ou réglementation, y compris celles applicables à la personne concernée. »

© Hervé Schauer Sécurité

Processus de gestion des risques

Déclaration d'applicabilité (DdA)

- Déterminer quelles mesures sélectionner
  - → Annexe A et/ou Annexe B de l'ISO27701 ?
- En amont de l'Appréciation et du Traitement des risques
  - → Lors de l'établissement du contexte

Réf. ISO27701 5.2.1 Compréhension de l'organisation et de son contexte

« L'organisation doit déterminer son rôle comme RT de TDCP (y compris comme responsable conjoint de traitement) et/ou comme ST de DCP ».

« Lorsque l'organisation agit dans les deux rôles, les différents rôles doivent être déterminés, chacun d'entre eux faisant l'objet d'un série de mesures distinctes ».

© Hervé Schauer Sécurité

Processus de gestion des risques

Déclaration d'applicabilité (DdA)

- Qui est le propriétaire des risques ?
- Qui doit approuver le PTR ?
- Qui doit accepter les risques résiduels ?

PIA (CNIL) :

- Les DPO donne un avis
- Seul de RT peut valider le PIA

La norme ISO29134 précise :

- En plus de l'approbation du PTR et de l'acceptation des risques résiduels

> « La responsabilité de la direction devrait également être obtenue en signant la déclaration d'acceptation. »

Faut-il adopter la même logique ?

Pas de précision dans la norme ISO27701.

Proposition

- Avis du DPO sur risques résiduels ayant des conséquences pour les PC et le volet Protection de la vie privée
- Validation des NC résiduelles par le RT ou le ST
- Engagement du RT (ou du ST) par la signature de la déclaration d'acceptation

© Hervé Schauer Sécurité

Merci de votre écoute,

Amélie PAGET

Consultante indépendante -
Protection des données personnelles

Formatrice HS2

HS2
Hervé Schauer Sécurité

© Hervé Schauer Sécurité