L’ensemble documentaire de la PSSI générique

Objectifs

- fournir des documents rédigés sur la base de risques identifiés
- pour les établissements n'ayant pas de PSSI ou les ressources pour entamer une démarche complète
  - fournir des documents répondant à la plupart des besoins
  - faciles à s'approprier
- pour les établissements ayant leur PSSI mais n'ayant pas de processus d'amélioration continue
  - pouvoir mettre en œuvre ce processus
  - affiner l'analyse
  - répondre aux besoins de l'établissement

Type de documents

- documents génériques
- documents d'aide à l'analyse de risque
- documents permettant l'amélioration continue et la transmission d'un information pertinente

Les documents génériques

- rédigés par le prestataire Fidens et remis en forme par le GT-PSSI
- documents quasiment utilisables tels quels
- certains chapitres sont à adapter à votre établissement :
  - nom de l'établissement
  - enjeux et missions
  - certaines dénominations
  - …
- ils doivent être approuvés par la gouvernance (par exemple le CA)

Les documents génériques (2)

- PMSI : politique de management de la sécurité de l'information (ou politique de gouvernance de la sécurité de l'information) :
  - document décrivant l'organisation de la SSI dans votre établissement (instances de révision, veille, etc.)
  - document d'une vingtaine de pages
- PSSI : politique de sécurité du système d'information :
  - document recensant l'ensemble des règles de sécurité à mettre en œuvre et validées par le chef d'établissement
  - document d'une soixantaine de pages

Les documents génériques (3)

- PGSSI : la politique générale de sécurité de la sécurité du système d'information
  - reprend les chapitres de la PSSI
  - ne reprend que les grands thèmes et ne détaille pas
  - adopter ce document revient à le considérer comme étant la PSSI, la PSSI devenant un document d'application

Les documents d'aide à l'analyse de risque

- gestion du projet analyse de risque :
  - plan de management
  - guide d'entretiens
  - notes de cadrage
  - planning projet
  - cartographie du SI

Les documents d'aide à l'analyse de risque (2)

- des documents d'aide à la réalisation des étapes suivantes d'une analyse de risques :
  - analyse du contexte
  - étude des besoins
  - étude des menaces

Amélioration continue

- dans l'esprit des normes ISO 27000
  - une déclaration d'applicabilité type
  - un plan d'action type dans la mise en œuvre d'un processus d'amélioration continue
- une matrice d'affectation des mesures ISO :
  - pour le choix des règles
  - orientée métiers pour rédiger des guides métiers de la sécurité de l'information
- les risques évoluent : vos mesures doivent aussi évoluer

Les normes ISO 27000 ?

- ISO 27001 : management de la sécurité de l'information (SMSI)
- ISO 27002 : guide de bonnes pratiques (développement des annexes de la 27001)
- ISO 27005 : appréciation des risques
- ISO 27003 : implémentation
- ISO 27004 : indicateurs du SMSI

Que contient la PSSI générique

- un rappel des enjeux de l'établissement
- un rappel des obligations réglementaires
- des mesures de sécurité issues de la norme ISO 27002
- ces mesures couvrent des risques identifiés lors des analyses
- ces mesures sont déclinées en règles les mettant en œuvre

Grands chapitres de la PSSI

- gestion de la politique
- gestion des biens (inventaires et attributions)
- sécurité liée aux ressources humaines
- gestion des tiers
- habilitation
- sécurité des échanges de données
- sécurité des réseaux
- sécurité des applications
- mobilité
- projets, développements et maintenance
- sauvegardes
- continuité d'activité
- gestion des incidents
- …

Exemples

Classification des biens

[ISO 27001 - A 7.2.1] Lignes directrices pour la classification

[GDB_01] Plan de classification

- Un plan de classification est défini au niveau de l'établissement pour hiérarchiser les niveaux de protection et gérer les biens conformément aux besoins de sécurité identifiés.
- Ce plan de classification définit les échelles de sensibilité à partir des critères confidentialité, intégrité, et disponibilité.

Exemples (2)

Inventaire des biens

[ISO 27001 - A 7.1.1] Inventaire des biens

[GDB_02] Identification et inventaire des biens sensibles

- On qualifie de « bien sensible » toute composante qui traite d'information ou de fonction de niveau 2 selon le plan de classification. On appelle « critique » un bien supérieur au niveau 3 selon le plan de classification.
- Les biens sensibles participant au fonctionnement du système d'information (informations, biens logiciels, biens physiques, services, etc.) sont inventoriés par domaine. Chaque bien recensé fait l'objet d'une identification renseignant le niveau de classification (établi sur la base du plan mentionné ci-dessus), son détenteur ou responsable, et les personnes qui y ont accès (pour les données).
- Un extrait de l'inventaire est réalisé afin d'identifier les biens « critiques » parmi l'ensemble des biens constituant le système d'information de manière à pouvoir protéger les éléments vitaux de l'organisme identifiés en cas de sinistre majeur.

Exemples (3)

Utilisation de matériel hors des locaux

[ISO 27001 - A 9.2.5] Sécurité du matériel hors des locaux

[NOMAD_05] Dispositifs de sécurité installés sur les nomades

- Tout poste nomade comprend par défaut :
  - Un antivirus / anti-spam.
  - Un logiciel de chiffrement de disque et/ou des fichiers.
- Selon les besoins identifiés et les informations traitées, des configurations durcies peuvent être mises à disposition des usagers : authentification forte pour la connexion au poste, outil de sécurisation de la connexion VPN, outil de chiffrement des disques durs, support amovible sécurisé, outil de contrôle de double connexion.

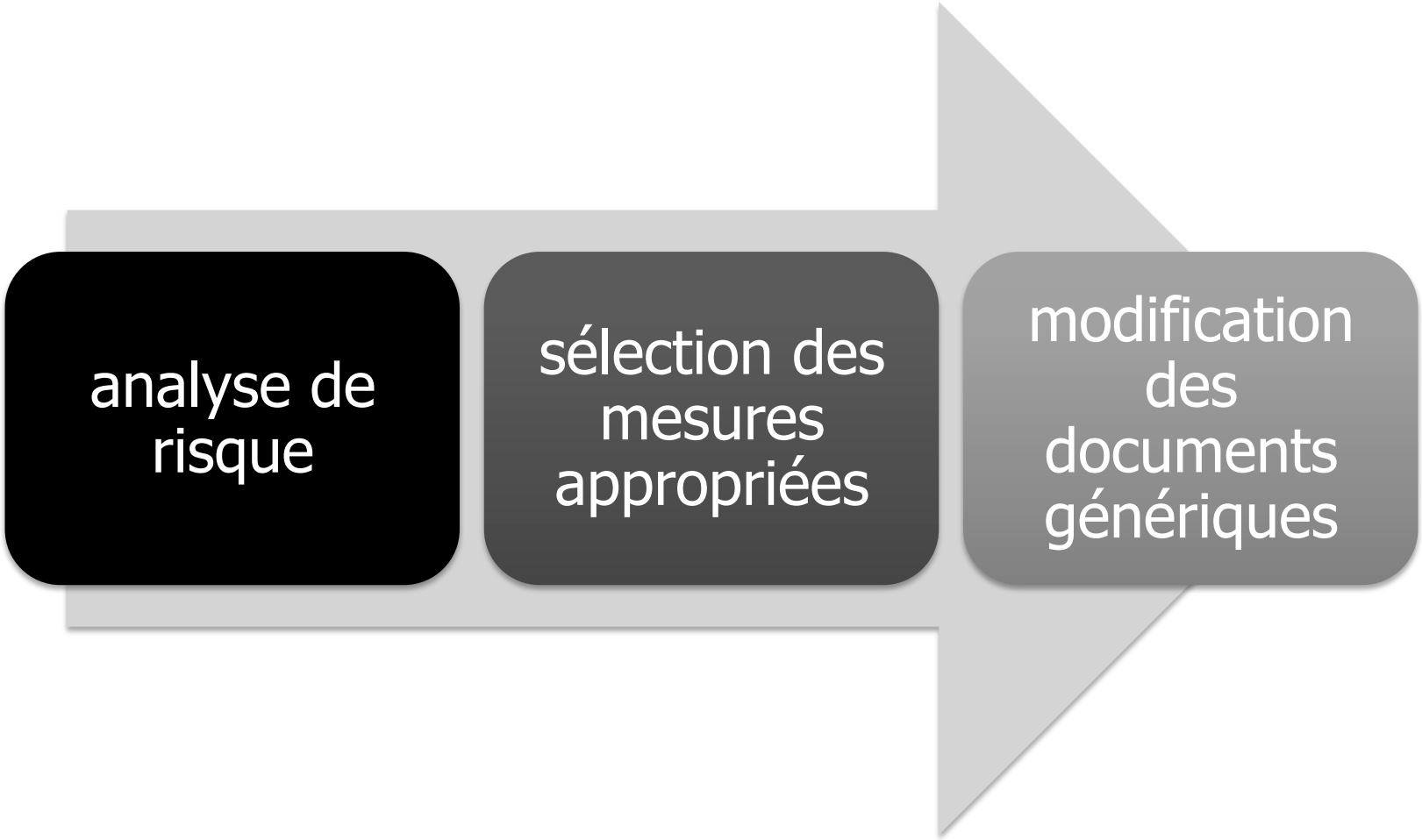
Plan de la PMSI

- 1. Introduction
- 2. Contexte
- 3. Grands principes
  - 3.1. Principes de gouvernance
  - 3.2. Principes de sécurité
- 4. Gestion des risques
  - 4.1. Stratégie
  - 4.2. Critères
  - 4.3. Audit et contrôle

Plan de la PMSI (2)

- 5. Organisation de la sécurité
  - 5.1. Le Comité de Pilotage Stratégique
  - 5.2. Le Comité de Sécurité Opérationnelle
  - 5.3. Les comités de liaison
  - 5.4. Fonctions présentes aux comités
  - 5.5. Rôles et responsabilités
- 6. Mesure et amélioration de la sécurité
  - 6.1. Amélioration du niveau de sécurité
  - 6.2. Amélioration du processus SMSI
  - 6.3. Gestion du document de politique SMSI

Démarche complète



Scénarios d'utilisation

- dans tous les cas :
  - un groupe projet (travail sur les documents et les entretiens)
  - un comité de pilotage : validation des travaux avant adoption
  - l'étude du contexte vous permettra :
    - d'identifier les missions et axes stratégiques de l'établissement
    - de définir le périmètre de la PSSI
    - définir les critères de gestion de risques

Scénarios d'utilisation (2)

- si vous avez peu d'énergie à consacrer à la démarche complète
  - travail sur les documents PMSI, PSSI (et PGSSI)
  - évaluation de l'applicabilité des règles proposées (organisation, finances,…)
  - adaptation des règles à votre contexte (ou retrait selon le cas)
  - validation des documents par les instances dirigeantes
  - planification de la mise en œuvre

Scénarios d'utilisation (3)

- si vous pouvez réunir une équipe projet sur une étude de risques :
  - reprendre les documents d'analyse de risques
  - réévaluer les besoins de sécurité
  - réévaluer la vraisemblance des menaces
  - appliquer une stratégie de traitement des risques
    - par les mesures : impacts financiers par exemple
    - par les risques (ex. : traitement des risques de niveau 3 et 4)
  - adapter alors les documents PMSI et PSSI

Scénarios d'utilisation (4)

- reprendre toute la démarche
- en partant ou pas des documents d'analyse de risque
- identification des mesures :
  - la matrice de correspondance permet de sélectionner les règles des documents génériques
- adapter alors les documents PMSI et PSSI

Important

- une équipe projet ayant un minimum de culture sur les études de risques
  - formations du CFSSI
  - formation 27000 ?
- une gouvernance impliquée
  - la sécurité est au service des intérêts de l'établissement
- c'est une culture qui s'acquiert par l'usage
  - commencer sur un périmètre plus restreint

Où trouver les documents ?

- intranet des RSSI de l'enseignement supérieur et de la recherche :
  - https://services.renater.fr/ssi/rssi/pssi/
- accès réservé, adressez-vous à votre RSSI pour les obtenir