Conseil et préconisations de mutualisation ISO 2700x et ISO 20000 /ITIL

Groupe de travail du Club 27001 Toulouse
Présentation du 3 février 2012

Nicole Genotelle, Joris Pegli,
Emmanuel Prat, Sébastien Rabaud

Agenda

- Introduction
- Rappels des travaux du premier groupe de travail
- Des éléments complémentaires sur les normes et guides de bonnes pratiques
- Objectifs et contexte de la présente étude
- Présentation de l'étude
- Conclusion
- Et pour la suite …

Introduction

- Nouveau groupe de travail ITIL du Club 27001, composé de quatre personnes du Club 27001 Toulousain.
- Le groupe se réunit depuis le mois d'août 2011 pour réactiver les travaux et les réflexions sur les mutualisations possibles entre les normes ISO27001 et ISO20000 (ITIL).
- Le groupe a tenu compte des travaux réalisés par l'ancien groupe de travail ITIL du Club 27001.

Rappels des travaux du premier groupe de travail

Objectif

- ✓ Fournir des fiches de mutualisation des services ITIL/ISO27001

Couverture

- ✓ ITIL concerne l'**informatique**
- ✓ ISO 27001 concerne l'**information** au sens large

Nature

- ✓ ITIL : **Bonnes pratiques** : aucun caractère contraignant
- ✓ ISO 27001: **Exigences** : obligation de tout mettre en œuvre entre les chapitres 4 et 8 de la norme

Analyses des travaux du premier groupe de travail

- Nos premières constatations nous amènent à préciser les éléments suivants :
  - ✓ **Nature**
    - ITIL : **Bonnes pratiques** : aucun caractère contraignant
    - ISO 20000 : **Exigences** : obligation de tout mettre en œuvre ⇨ Certification
    - ISO 27001: **Exigences**; obligation de tout mettre en œuvre entre les chapitres 4 et 8 de la norme ⇨ Certification
    - ISO 27002 : **Bonnes pratiques** : aucun caractère contraignant
  - ✓ **Les rapprochements possibles sont :**
    - ITIL et ISO 27002 : bonnes pratiques
    - ISO 20000 et ISO 27001 : objectifs de certification

Des éléments complémentaires

La norme ISO 27013 : Guidelines on the integrated implementation of ISO 27001 and ISO 20000-1 en cours de rédaction (1st Committee Draft 26/08/2011)

- ✓ C'est un guide d'optimisation de la mise en place simultanée des 2 démarches en vue d'une double certification,
- ✓ Elle contient une table de correspondances des chapitres entre 27001 et 20000
- ✓ Elle contient une comparaison du vocabulaire entre 27001 et 20000

  ⇨ attention aux faux-amis
- ✓ Elle ne fournit pas d'éléments dans le cas où les deux démarches seraient décorrélées dans le temps.

Apport de ITIL V3 par rapport à ITIL V2

- ✓ Extension de la base de données des connaissances à l'ensemble des informations IT,
- ✓ Périmètre étendu,
- ✓ Prise en compte du cycle de vie complet du service de sa conception à sa disparition.

Objectifs et contexte de la présente étude

Hypothèse

- ✓ Pré-existence d'un processus ITIL définit dans l'entreprise et volonté de mise en place d'une démarche sécurité

Objectifs

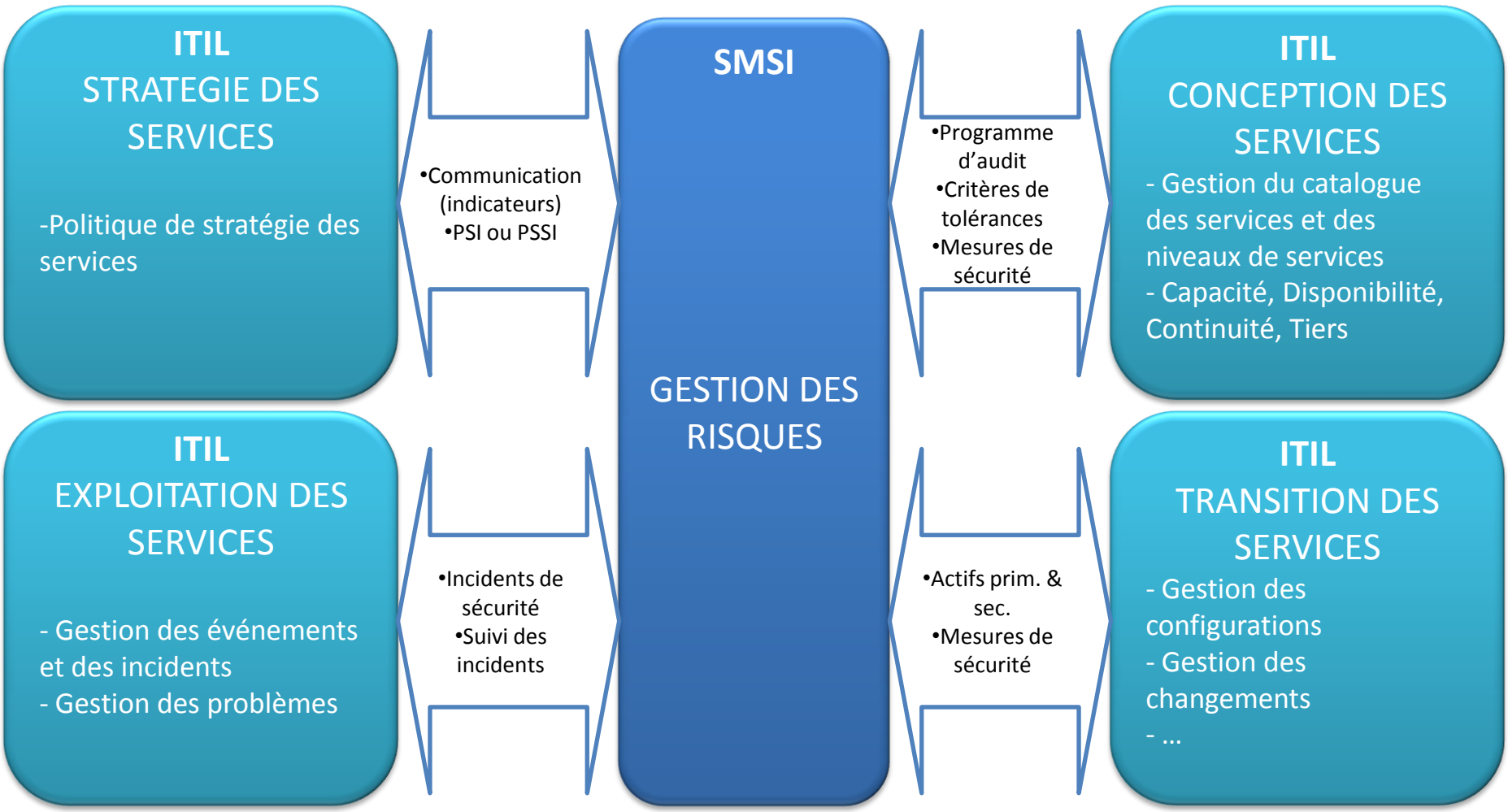
- ✓ Identifier les apports réciproques des processus ITIL et du processus cœur du SMSI : la gestion des risques
- ✓ Identifier les points d'amélioration ou d'adaptation des pratiques ITIL

⇒ Réaliser une analyse pragmatique de mutualisation de la démarche de mise en place de ISO27001 // aux bonnes pratiques ITIL

Contexte

- ✓ Prise en compte d'ITIL V3
- ✓ Pas de comparaison ISO27001 & ISO20000 ⇨ la norme ISO27013 en cours de rédaction/validation traite déjà ce sujet

Vision globale des apports réciproques



Processus ITIL : Politique de stratégie des services

Apports ITIL ⇨ SMSI

- ✓ Contribution à la définition du périmètre, du contexte et des enjeux sécurité

⇒ Contribution pour la PSI ou PSSI

Apports SMSI ⇨ ITIL

- ✓ Communication : mise à disposition d'indicateurs sécurité en cohérence avec les exigences des contrats (OLA, SLA)

Conseils / préconisations

- ✓ Ne pas se limiter au périmètre ITIL (informatique) pour définir celui du SMSI (information)
- ✓ Qualité et pertinence des indicateurs : « décisionnel »

Processus ITIL : Gestion du catalogue et des niveaux de service

Apports ITIL ⇨ SMSI

- ✓ Compléter le programme d'audit
- ✓ Définir le niveau de tolérance aux risques DICT
- ✓ Définir les indicateurs du tableau de bord sécurité

Apports SMSI ⇨ ITIL

- ✓ Accompagnement à la maîtrise des OLA : intégration des niveaux de tolérance aux risques DICT

Conseils / préconisations

- ✓ Intégration de la sécurité dès la conception des services :
  - Etablissement d'un contrat de service OLA entre les ≠ responsables des processus ITIL et le responsable du processus sécurité

    Exemple : Le responsable du processus de gestion des changements informe le responsable du processus de sécurité des modifications

    ⇨ Permet d'évaluer l'impact des changement sur la sécurité
- ✓ Dans ITIL : Le niveau de service est souvent limité au seul critère de Disponibilité
- ✓ Visibilité de la sécurité par le client :
  - Adapter le niveau de sécurité à la demande client (SLR dans ITIL)

  ⇨ À intégrer dans les OLA (contrat de service interne) / SMSI

  ⇨ Eventuellement dans les SLA (contrat de service client si spécifié dans les SLR)

Processus ITIL : Gestion des capacités, de la disponibilité, de la continuité, des tiers

Apports ITIL ⇨ SMSI

- ✓ Recensement des mesures de sécurité avec leurs niveaux de maturité et d'efficience
- ✓ Contribution au programme d'audit
- ✓ Contribution à la rédaction du PCA

Apports SMSI ⇨ ITIL

- ✓ Mise à jour du plan de traitement des risques et des indicateurs sécurité

Conseils / préconisations

- ✓ Limite du périmètre ITIL (informatique) ≠ SMSI (information)

Processus ITIL : Gestion des configurations (CMDB)

Apports ITIL ⇨ SMSI

- ✓ Support pour la définition et le suivi des actifs du SMSI
- ✓ Approche PDCA en continu ⇨ plan de traitement des risques
- ✓ Identification des actifs en support (27005) bien support (EBIOS) à partir de la CMDB
- ✓ S'appuyer sur la CMDB pour les activités sécurité (périmètre de la veille, actifs servant à l'analyse de risque liées aux vulnérabilités courantes)

Apports SMSI ⇨ ITIL

- ✓ Enrichissement de la CMDB (type des actifs primordiaux ou secondaires, niveau de tolérance DICT)
- ⇨ Cf. ISO20000-2- 9.1.2.NOTE ⇨ « other items that may be considered as CI : people, business units, other assets, facilities… »

Conseils / préconisations

- ✓ Fonctionnalités limitées de certain outil de la CMDB,
- ✓ Niveau de finesse du contenu dans la CMDB a bien calibrer (assez d'information pour être pertinent mais pas trop pour ne pas avoir de mise à jour continuelle)

Processus ITIL : Gestion des changements

Apports ITIL ⇨ SMSI

- ✓ L'évolution du système peut être relayé en continu vers la sécurité
- ✓ Approche PDCA en continu => réévaluation ou instanciation de nouveaux scénarii

Apports SMSI ⇨ ITIL

- ✓ Mise à jour du plan de traitement des risques et des indicateurs sécurité

Conseils / préconisations

- ✓ Implication non naturelle du RSSI dans la gestion des changements
- ⇨ Adaptation des procédures de management (PAQ, PMP, …), si possible de la politique de stratégie des services

Processus ITIL : Evaluation des changements, validation/tests, recettes, mises en production

Apports ITIL ⇨ SMSI

- ✓ Liste des mesures de sécurité avec leurs niveaux de maturité et d'efficience
- ✓ Mise à jour du programme d'audit
- ✓ La présence de champs DICT dans la CMDB facilite la priorisation de la gestion des patchs de sécurité

Apports SMSI ⇨ ITIL

- ✓ Mise à jour du plan de traitement des risques et des indicateurs sécurité

Conseils / préconisations

- ✓ Limite du périmètre ITIL (informatique) ≠ SMSI (information)

Processus ITIL : Gestion des événements et des incidents

Apports ITIL ⇨ SMSI

- ✓ Identification des incidents de sécurité parmi les incidents remontés par le processus gestion des incidents (Analyse à postériori et si possible en temps réel)
- ✓ La présence de champs DICT dans la CMDB facilite la priorisation de la gestion des évènements et des incidents
- ✓ Approche PDCA en continu ⇨ réévaluation ou instanciation de nouveaux scénarii

Apports SMSI ⇨ ITIL

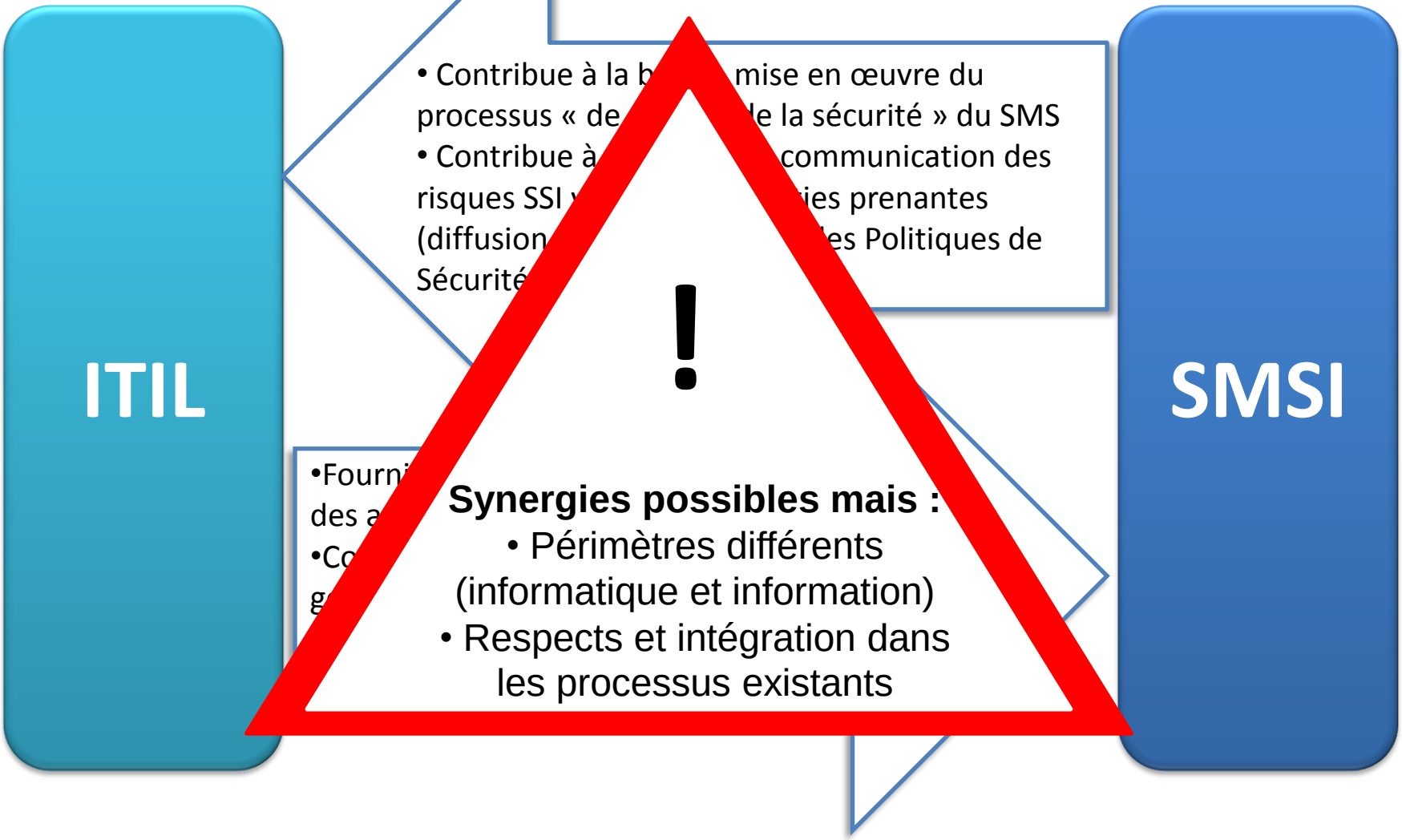
- ✓ Mise à jour du plan de traitement des risques et des indicateurs sécurité

Conseils / préconisations

- ✓ Difficulté à adapter le processus de qualification des incidents pour permettre l'identification exhaustive des incidents de sécurité
- ✓ Compétences des opérateurs en générale insuffisante ou inefficace pour identifier les évènements de sécurité

⇨ rôle du Responsable du centre de service « tour operator » plus adapté ?

Conclusion


ITIL
SMSI
• Contribue à la b mise en œuvre du processus « de le la sécurité » du SMS
• Contribue à communication des risques SSI ies prenantes (diffusion es Politiques de Sécurité
•Fourni
des a
•Co
g
!
Synergies possibles mais :
• Périmètres différents (informatique et information)
• Respects et intégration dans les processus existants

Et pour la suite …

Retours d’expérience ?