S

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

Groupe de travail du Club 27001 Toulouse
3 Avril 2012

Nicole Genotelle (ON-X / Edelweb), Joris Pegli (SRC-Solution),
Emmanuel Prat (FullSave), Sébastien Rabaud (SCASSI Conseil),
Jacques Sudres (C&S)

Agenda

- Introduction
- Constats du premier groupe de travail
- Analyses et compléments
- Ce qui a changé
- Contexte et objectifs du groupe de travail
- Présentation de l'étude
- Conclusion
- Et pour la suite …

Introduction

- Nouveau groupe de travail ITIL du Club 27001, composé de cinq 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.

Premier groupe de travail

Objectif

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

Couverture

- ✓ ITIL concerne l'**informatique**
- ✓ ISO 27001 concerne l'**information**

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

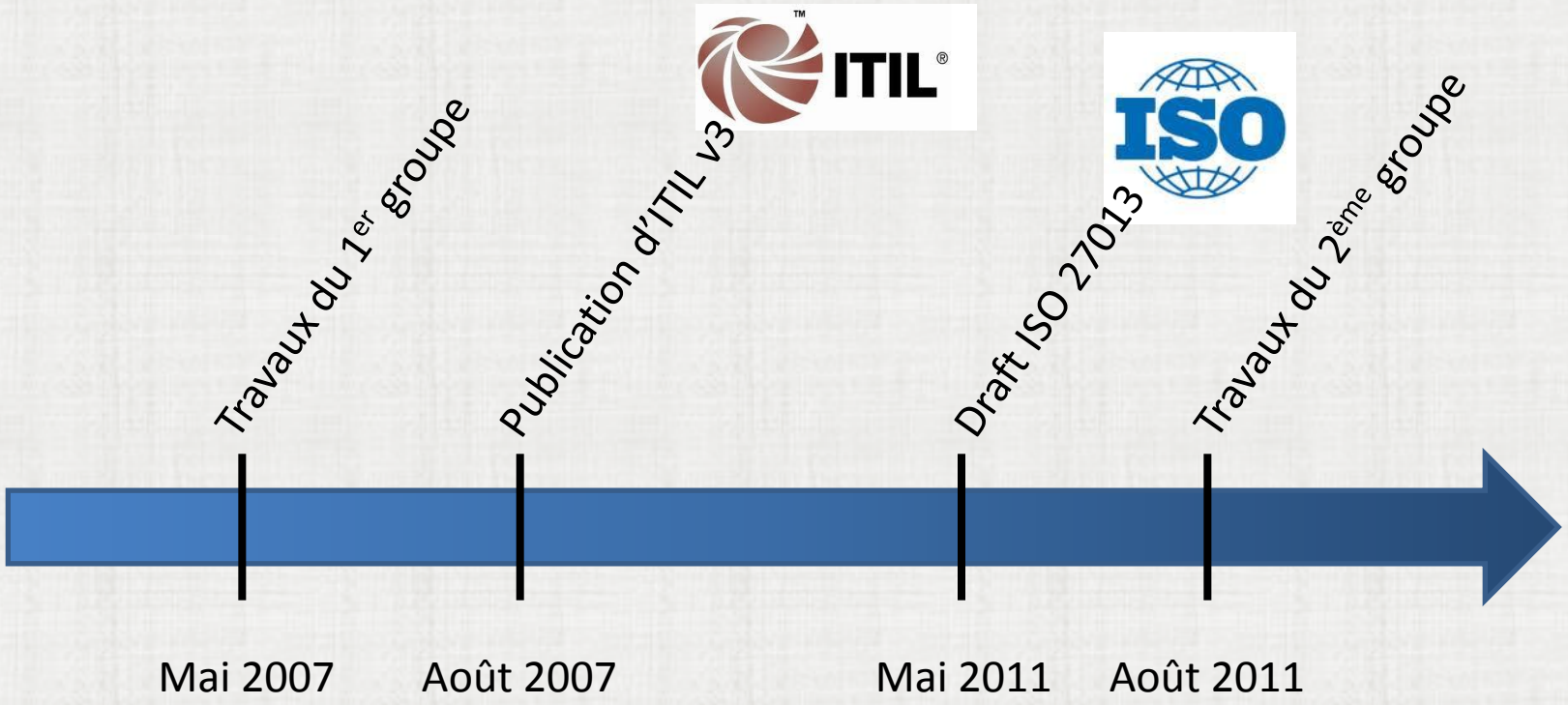
Analyse et compléments

Domaines	Exigences	Bonnes pratiques
Services informatiques	ISO 20000	ITIL
Sécurité de l'information	ISO 27001	ISO 27002

✓ **Les rapprochements possibles sont :**

- ITIL et ISO 27002 : bonnes pratiques
- ISO 20000 et ISO 27001 : objectifs de certification

Ce qui a changé …



Ce qui a changé …

ISO 27013	***Guideline**s on the integrated implementation of ISO 27001 and ISO 20000-1 - En cours de validation (40.20 – enquête / mise au vote – 15/11/2011)* ✓Guide d'optimisation de la mise en place simultanée des 2 démarches en vue d'une double certification, ✓Table de correspondances entre les chapitres 27001 et 20000 ✓Comparaison du vocabulaire entre 27001 et 20000 => Divergence ▪ ISO27001 : Distinction entre événements et incidents (liés à la sécurité de l'information) ▪ ISO20000 : Tout évènement est un incident (pas de définition d'évènement) ✓Pas d'éléments dans le cas où les deux démarches seraient décorrélées dans le temps.
ITIL V3	✓Prise en compte du cycle de vie complet du service de sa conception à sa disparition. ✓Le processus central devient « Le catalogue de services » à la place de la CMDB ✓Extension de la base de données des connaissances à l'ensemble des informations IT, ✓Les processus font tous référence au service

Contexte et objectifs du groupe de travail

Hypothèses

- ✓ Préexistence de processus ITIL
- ✓ Prise en compte d'ITILv3
- ✓ Pas de comparaison ISO27001 & ISO20000 ⇨ ISO27013

Objectifs

- ✓ Identifier les processus ITIL utiles dans le cadre de la mise en œuvre d'un SMSI
- ✓ Identifier les adaptations des processus ITIL induites par la mise en œuvre du SMSI

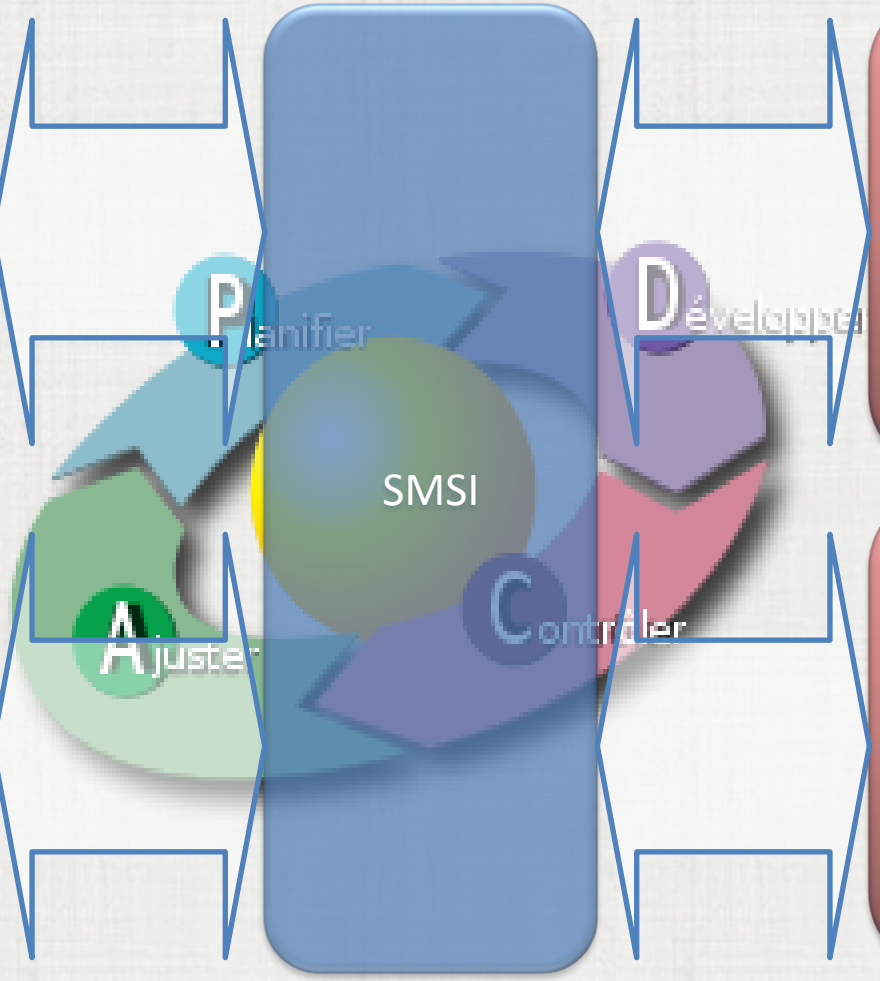
Démarche

- ✓ Analyse des points de convergence avec le cycle de vie et les processus ITIL

Vision globale

ITIL
STRATEGIE DES SERVICES

ITIL
CONCEPTION DES SERVICES



ITIL
EXPLOITATION DES SERVICES

ITIL
TRANSITION DES SERVICES

Politique de stratégie des services

ITIL
-
Stratégie des Services
-
Politique de stratégie des services

✓ Contribue à la définition du périmètre, du contexte et des enjeux du SMSI (PSI, ….)

✓ Contribue à l'amélioration de la communication des risques SSI vis-à-vis des parties prenantes (diffusion / prise en compte des politiques de sécurité, etc.)

SMSI

☞ **Conseils / préconisations**

- ✓ Ne pas se limiter au périmètre ITIL (informatique) pour définir celui du SMSI (information)
- ✓ Qualité et pertinence des indicateurs niveau stratégique

Gestion du catalogue et des niveaux de service

ITIL
-
Conception des services
-
Catalogue
Niveaux de service

- ✓ Permet de prendre en compte dans le SMSI les niveaux de tolérance déjà définis dans ITIL
- ✓ Permet de prendre en compte des indicateurs déjà définis (niveau opérationnel)
- ✓ Permet de recenser les services de sécurité offerts

- ✓ Permet de prendre en compte dans les niveaux de tolérance ITIL les critères de sécurité définis par le SMSI
- ✓ Meilleure visibilité de la sécurité par les clients (SLA, OLA et UC)

SMSI

Gestion du catalogue et des niveaux de service

Conseils / Préconisations

- ✓ En pratique, le niveau de service est souvent limité au seul critère de Disponibilité (bien qu'ITIL prenne en compte également I et C).
- ✓ Intégrer la sécurité dès la conception des services :
  - Contrat de service OLA entre les ≠ responsables des processus ITIL et le responsable du SMSI

    Exemple : *la gestion des changements implique systématiquement les acteurs SSI :*

    - ⇨ *Prise en compte des changements sur la sécurité (mise à jour du risque)*
    - ⇨ *Sécurité dans les changements (tests de non-régression)*
- ✓ Adapter le niveau de sécurité à la demande client (SLR dans ITIL)
  - Intégrer dans les OLA (contrat de service interne) les exigences du SMSI
  - Éventuellement dans les SLA (contrat de service client si spécifié dans les SLR)

Gestion des capacités, de la disponibilité, de la continuité, des fournisseurs

ITIL
-
Conception des services
-
Capacités
Disponibilité
Continuité
Fournisseurs

✓ Permet de recenser les mesures de sécurité existantes avec leurs niveaux de maturité (capacité)
✓ Contribue à l'identification des tiers (fournisseurs)
✓ Contribue au PCA (continuité)

✓ Permet de prendre en compte l'évaluation des risques (continuité, disponibilité, fournisseurs, capacité)
✓ Permet de prendre en compte les exigences de sécurité vis à vis des tiers (fournisseurs)

SMSI

Conseils / préconisations

- ✓ Limite du périmètre ITIL (informatique) ≠ SMSI (information) [ex : Continuité]
- ✓ Limite du périmètre Fournisseurs (ITIL) ≠ Tiers (SMSI)

Gestion des actifs et des configurations

ITIL
-
Transition des services
-
Actifs
Configurations

✓ CMDB contribue à l'identification des actifs en support (27005)
✓ CMDB contribue à certaines activités sécurité : périmètre de la veille, actifs servant à l'analyse de risque liées aux vulnérabilités courantes, ..
✓ Approche PDCA en continu : prise en compte des mises à jour de la CMDB dans la gestion des risques

SMSI

✓ Enrichissement de la CMDB : type des actifs primordiaux ou en support, niveau de tolérance DICT, …

Conseils / préconisations

- ✓ Niveau de finesse du contenu dans la CMDB à bien calibrer (assez d'information pour être pertinent mais pas trop pour ne pas avoir de mise à jour continuelle)
- ✓ CMDB est susceptible d'intégrer tous types d'actifs. Cf. ISO20000-2-§9.1.2.NOTE ⇨ « other items that may be considered as CI : people, business units, other assets, facilities… »

Gestion des changements et mises en production

ITIL
-
Transition des services
-

Changements

Mises en production

✓ Permet de prendre en compte de manière continue les évolutions du SI (mise à jour gestion des risques, périmètre de la veille, …)
✓ La présence de champs DICT dans la CMDB contribue à l'évaluation des risques liés aux changements,

SMSI

✓ Prise en compte de la sécurité dans la gestion des changements (ex : tests de non régression)
✓ Permet de définir les priorités des demandes de changement (ex : changement urgent pour une vulnérabilité critique)

Conseils / préconisations

- ✓ Implication nécessaire des acteurs SSI dans la gestion des changements ⇨ adaptation des contrats de services internes (OLA) et des procédures de gestion des changements

Gestion des événements, incidents et problèmes

ITIL
-
Exploitation des services
-
Évènements
Incidents
Problèmes

✓ Contribue à identifier des évènements et incidents de sécurité parmi les évènements et incidents du SI

✓ Contribue à définir des mesures de prévention de l'occurrence des incidents de sécurité (problèmes)

✓ Prise en compte des mesures liées aux incidents de sécurité (ex : identification systématique des incidents de sécurité, analyse et traitement des incidents à posteriori, …)

SMSI

Conseils / préconisations

- ✓ Difficulté à adapter le processus de qualification des incidents (à priori et à posteriori) pour permettre l'identification exhaustive des incidents de sécurité
- ✓ Compétences des opérateurs en général insuffisante ou inefficace pour identifier les évènements de sécurité

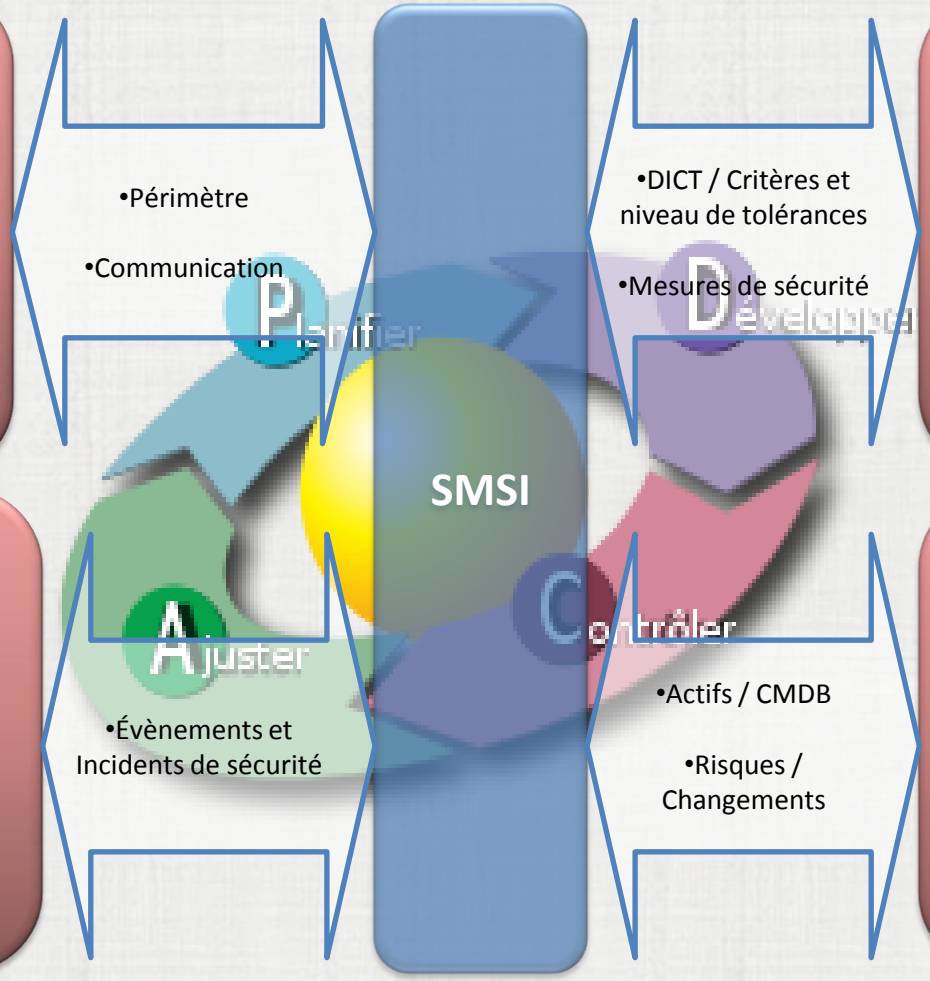
Conclusion

ITIL
STRATEGIE DES SERVICES

-Politique de stratégie des services

ITIL
CONCEPTION DES SERVICES

- Catalogue et niveaux de services
- Capacités, Disponibilité, Continuité, Fournisseurs



ITIL
EXPLOITATION DES SERVICES

- Événements
- Incidents
- Problèmes

ITIL
TRANSITION DES SERVICES

- Actifs, Configurations
- Changements, MEP

Conclusion

- Périmètre différent : Informatique ≠ Information
- Efficacité de la mutualisation dépendante de la maturité d'ITIL :
  - Nombre de processus ITIL
  - Maturité des processus
- Comment positionner « la sécurité » vis-à-vis d'ITIL ?
  - Comme un métier (externe) => SLA
  - Entièrement intégrée dans les processus ITIL => OLA
  - Existant en termes de processus et organisation?

Et pour la suite …

Approfondir des thématiques :
changements, incidents, etc. ?