



Opportunités de mutualisation ITIL et ISO 27001

**Clusir Rhône Alpes
Club SSI
Lyon, 30 janvier 2008**

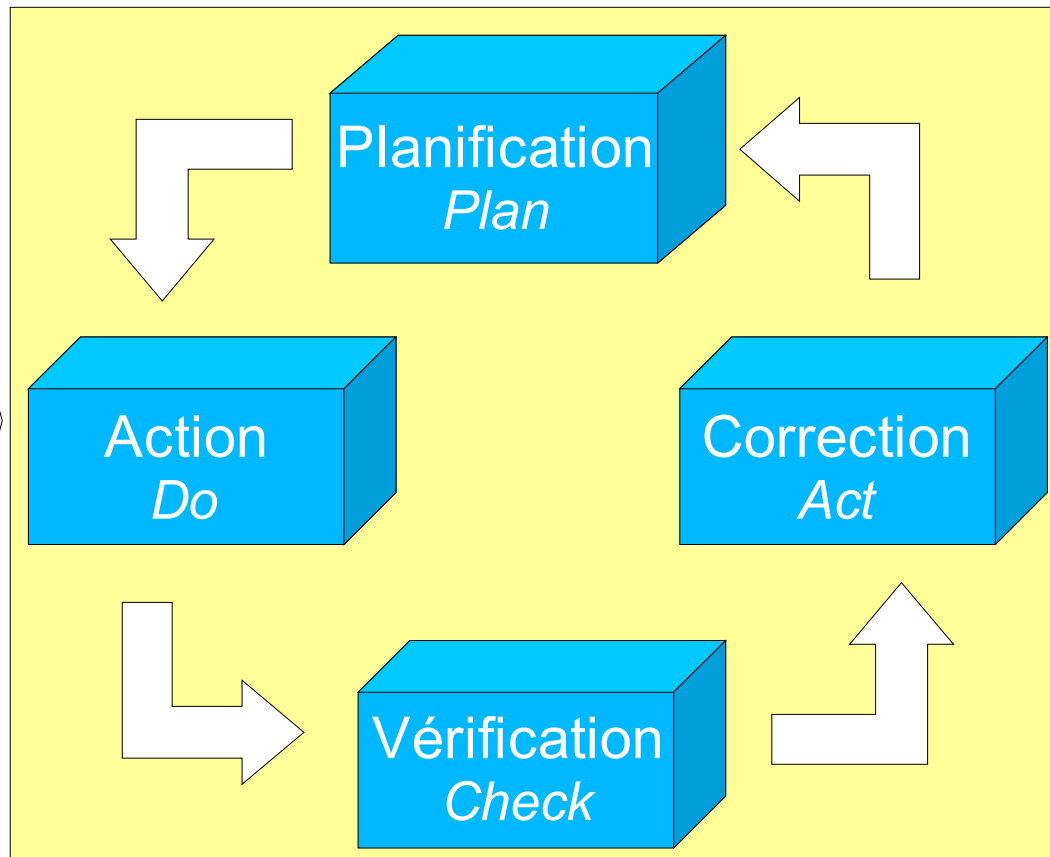
Alexandre Fernandez-Toro
<Alexandre.Fernandez-Toro@hsc.fr>

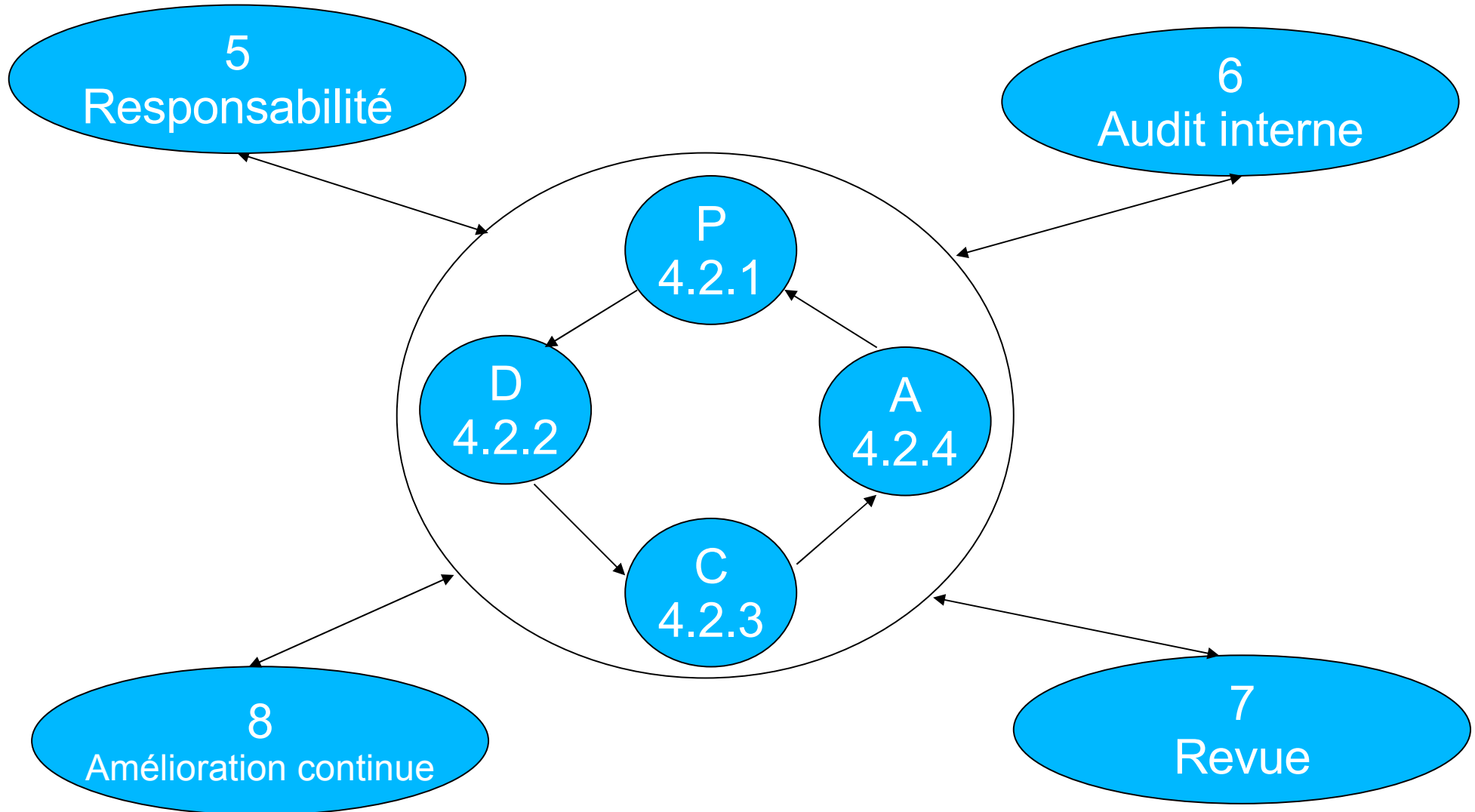
- Norme précisant les exigences pour
 - La mise en place
 - L'exploitation
 - L'amélioration
- d'un SMSI.
- Clauses 4 à 8
 - Obligatoires
 - Pas d'exceptions permises
- Mesures de sécurité de l'annexe A
 - Sélection en fonction du traitement du risque

Attentes et exigences en terme de sécurité

Modèle **PDCA** : Plan-Do-Check-Act

Sécurité effective fournie





- En suivant la norme...
 - Périmètre et Politique du SMSI
 - Inventaire des actifs
 - Appréciation des risques
 - Traitement du risque
 - Déclaration d'applicabilité (SoA)
 - Documentation
 - Mise en place des mesures de sécurité
 - Audit interne
 - Etc.

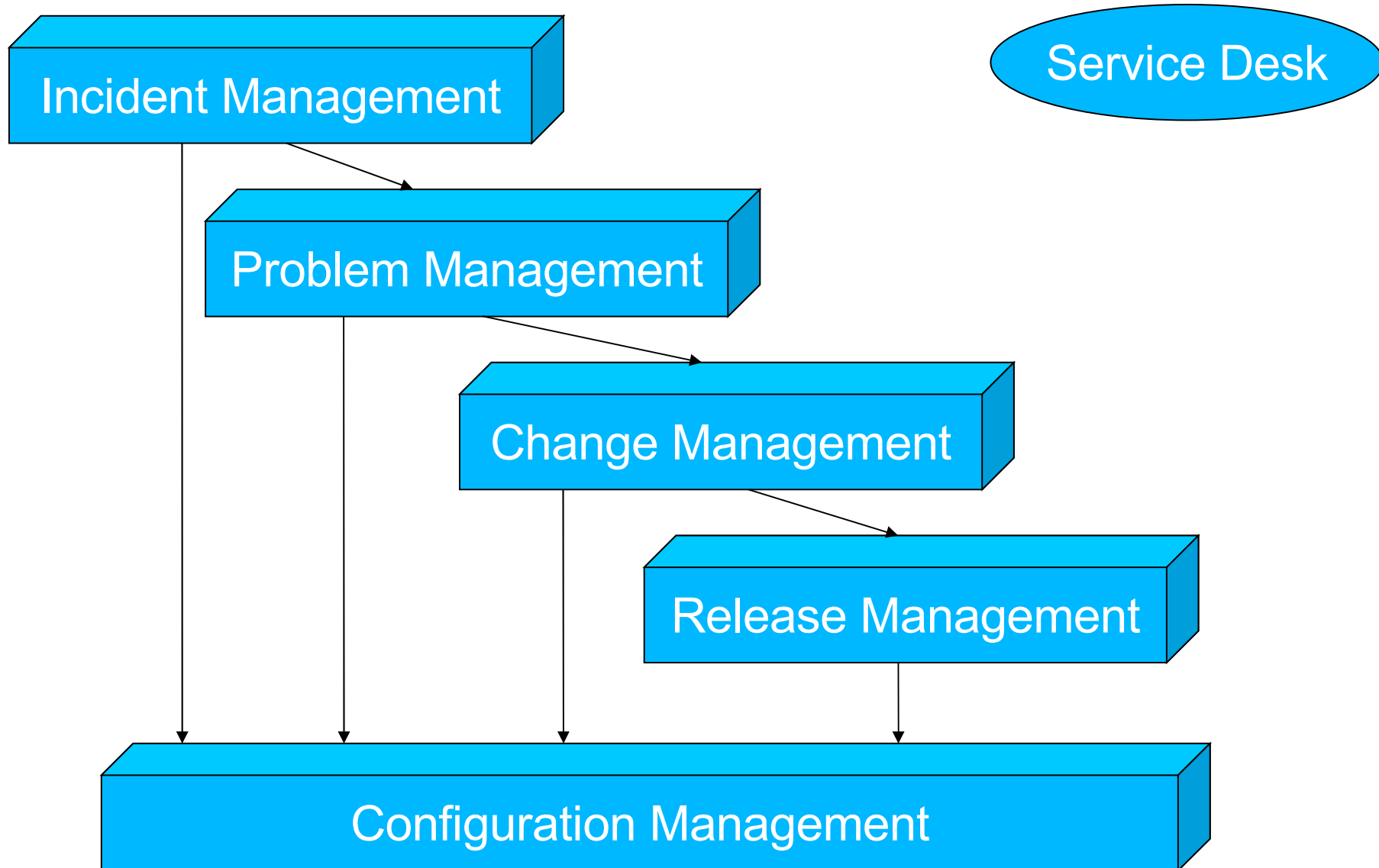
- Dans la vie réelle...
 - Etat des lieux ISO 27001
 - Rétro-analyse des risques
 - Politique et périmètre
 - Re-analyse des risques
 - « *PDCA-tisation* » des mesures de sécurité
 - Mise en place des mesures de sécurité manquantes

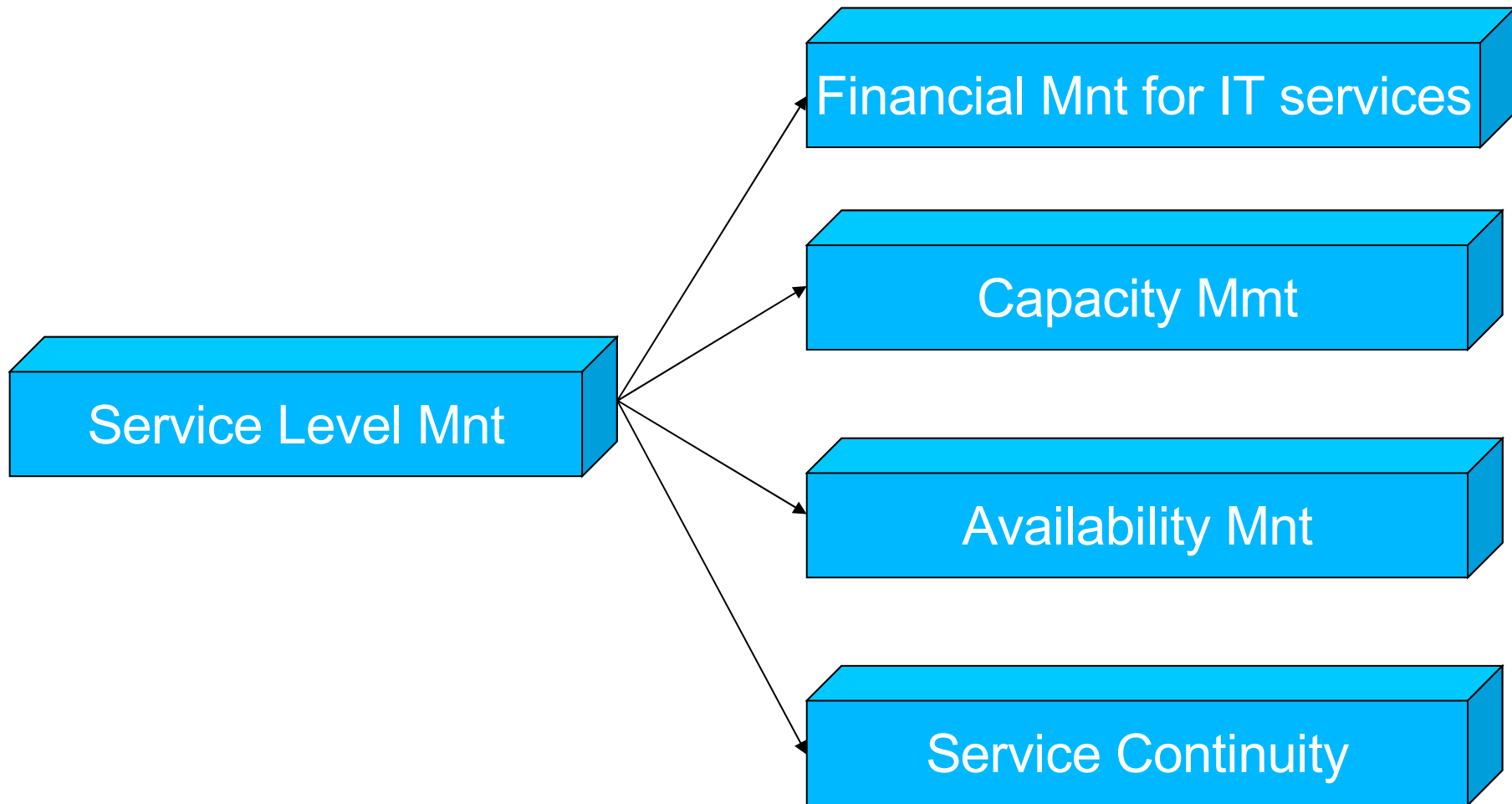
- Difficultés les plus communes
 - Inventaire des actifs
 - Appréciation des risques
 - Gestion de la documentation
 - Suivi des actions
 - Correctives
 - Préventives

- Difficultés les plus communes
 - Répartition des responsabilités avec les tiers
 - Sous-traitants
 - Maison mère
 - Détection d'incident
 - Comment le détecter ?
 - A qui le signaler ?
 - Gouvernance de la sécurité
 - Quelles instances de décision faut-il mettre en place?

- On parle souvent d'ITIL pour contribuer à régler ces difficultés
- Démarche
 - Présentation d'ITIL
 - Correspondances entre ITIL et l'ISO 27001
 - Opportunités de mutualisation ITIL et ISO 27001
 - Voies de recherche

- ITIL
 - Information Technology Infrastructure Library
 - Ensemble de bonnes pratiques en matière de gestion de services informatiques
 - Créé par l'administration britannique
 - Orienté business
 - Processus transversaux
 - Couvre 7 domaines → 7 livres





Service Desk

Configuration Mmt

4.2.1.d 1 Identify information assets

Incident Management

4.2.2.h Prompt detection & response to security events et 4.2.3 a 1 et 2

Problem Management

7.2 e Vulnérabilités non encore traitées
8.2 Corrective action

Change Management

8.2 Corrective action
8.3 Preventive action

Release Management

Service Desk

13.1.1. reporting information security events
13.1.2. reporting security weaknesses

Configuration Mmt

7.1.1. Inventory of assets
15.1.2. Intellectual property rights

Incident Management

Problem Management

13.2.2. Learning from information security incidents

Change Management

10.1.2. Change management
10.1.4. Sepatation of dev, test and operational facilities

Release Management

12.5.1. Change control procedures
12.5.2. Tech review of appl after OS change

Service Level Mnt

Financial Mnt for IT services

Availability Mnt

Capacity Mmt

Service Continuity Mmt

4.2.2. a Risk treatment plan
5.1 e Providing sufficient resources to establish, implement, operate [...] the ISMS

Service Level Mnt

10.2.1. Service delivery
10.2.2. Monitoring and review
of third party services

Financial Mnt for IT services

Availability Mnt

9.2. Equipment security
Entre autres...

Capacity Mnt

10.3.1. Capacity management

Service Continuity Mnt

14. Business continuity management

- Inventaire des biens
 - Notion de CMDB
 - Activités relatives au Configuration Management
 - Planification du Configuration Management
 - Identification des CI
 - Périmètre, niveau
 - Obtenir les informations
 - Formaliser les relations entre CI
 - Contrôle
 - Enregistrement, archivage, mise à jour
 - Vérification et audit

- Différents types de CI
 - Hardware, network components
 - software
 - business systems - custom-built applications
 - physical databases
 - software releases
 - configuration documentation, licences, maintenance agreements, SLA,
 - other resources e.g. users, suppliers, contracts
- Pas de notion de locaux

- Attention aux points suivants
 - Types de CI concernés par le SMSI (personnes, locaux, etc).
 - Il faut un RFC (request for change) chaque fois qu'il y a un changement
 - Niveaux de finesse de la CMDB et de l'inventaire des biens
 - Trop fin → Trop de MAJ
 - Trop gros → Modélisation inutile
 - Périmètres du SMSI et d'ITIL
 - Le périmètre du SMSI peut être plus vaste que le périmètre d'ITIL

- Détection d'incidents
 - Situation courante
 - Souvent, lorsque l'on met en place l'ISO 27001 il n'y a pas de démarche formelle de détection et réaction aux incidents
 - Exigence concernée
 - 4.2.2. h « Implement procedures [...] to security incidents. »
 - A.13 Information security incident management

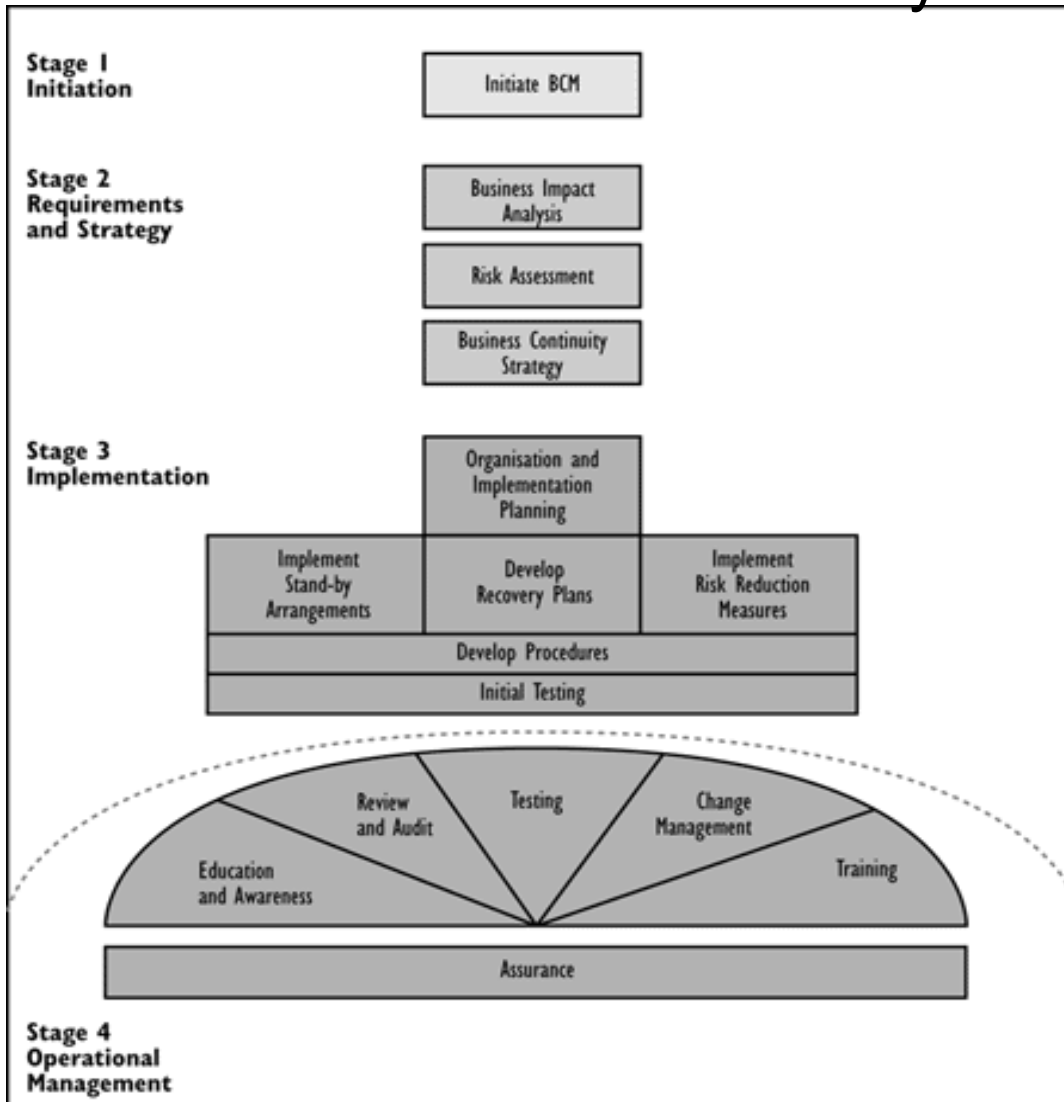
- Approche ITIL
 - Activités
 - Détection et enregistrement
 - Classification
 - Enquête et diagnostic
 - Résolution
 - Fermeture
 - Donne lieu à la génération de RFC (*request for change*)
 - Interagit avec la CMDB
 - Notion de « *known error* » et de « *workaround* »

- Suivi d'actions correctives et préventives
 - Situation courante
 - Pas de suivi formel des actions correctives et préventives
 - Exigence de l'ISO 27001
 - 4.2.4 *Maintain and improve ISMS*
 - 8 *ISMS Improvement*
 - Plusieurs processus ITIL sont concernés
 - Configuration Mt: *Incident* ↔ *Change* ↔ *Release*
 - *Service level Management*
 - *Service Improvement Program*

- Gouvernance
 - Situation courante
 - Pas d'instance pour officialiser les décisions
 - On ne sait pas quelles instances créer (comités)
 - Exigences de l'ISO 27001
 - Notion de « *approved by management* » omniprésente
 - A 6.1.1 *Management commitment do information security*
 - A 6.1.2 *Information security coordination*
 - A 6.1.3 *Allocation of information security responsibilities*

- Gouvernance
 - Approche ITIL sur l'exemple de la gestion du changement
 - Notion de RFC
 - Catégories de changement
 - Standard, Mineures, Majeures, Urgentes
 - Rôles
 - *Change manager*
 - *Change Advisory Board*
 - *CAB/ EC Emergency committee*
 - *Forward Schedule of changes (FSC)*
 - *Projected Service availability (PSA)*

ITIL : IT Service continuity



27001 : Business continuity Mt

- *A.14.1 Including information security in the BCM process*
- *A.14.1.2 Business continuity and risk assessment*
- *A.14.1.3 Developing and implementing continuity plans*
- *A.14.1.4 Business continuity planning framework*
- *A.14.1.5 Testing, maintaining and reassessing BCP*

- Relations avec les tiers
 - Situation courante
 - Les relations avec les sous traitants ne sont pas formalisées
 - La maison mère n'est pas perçue comme un fournisseur de services
 - Mesures de sécurité concernées
 - A.6.2 *External parties*
 - A.10.2 *Third party service delivery management*

- Relations avec les tiers
 - Approche ITIL
 - *Service catalogue*
 - *Service Level Requirements*
 - Analyse des risques
 - SLA
 - *Underpinning contracts (UC)*
 - *Operational Level Agreement (OLA)*

- Il existe bien des correspondances mais
 - Il y a des « faux amis »
 - Il y a des « vrais amis »
 - Il y a des exigences ISO 27001 couvertes par plusieurs processus ITIL
 - Il y a des exigences ISO 27001 couvertes par tous les processus ITIL
 - Il y a presque toujours des nuances entre les processus ITIL et ISO 27001
- → La mutualisation ITIL / ISO 27001 est moins triviale qu'elle n'en a l'air

- Ressemblances entre ITIL et ISO 27001
 - Une origine culturelle anglo-saxonne
 - Une approche PDCA
 - Explicite et systématique dans l'ISO 27001
 - Omniprésente dans ITIL
 - De nombreux points communs
 - Donc, d'importantes opportunités de mutualisation

- Attention aux dissemblances
 - Objectif
 - ITIL : Fournir au client un service orienté business
 - ISO 27001 : Fournir aux parties prenantes la confiance en matière de sécurité de l'information
 - Couverture
 - ITIL concerne l'informatique
 - C'est le « IT » de ITIL
 - ISO 27001 concerne l'Information au sens large
 - Nature
 - ITIL = Bonnes pratiques → Aucun caractère contraignant
 - C'est le « IL » de ITIL
 - ISO 27001 = Exigences → Obligation de tout mettre en œuvre entre les chapitres 4 et 8 de la norme

- Trois approches de mutualisation
 - ISO 27001 → ITIL
 - Il y a un intérêt...
 - ...mais il me paraît limité.
 - ITIL → ISO 27001
 - Tout dépend des processus ITIL qui sont déjà en place
 - Attention au niveau de finesse de la CMDB
 - Ne pas oublier les points abordés par ISO 27001 et non abordés par ITIL (Sécurité physique, ressources humaines, etc...)
 - Mettre en place ITIL et ISO 27001 en parallèle
 - Solution optimum, à mon avis...
 - ...mais ne pas oublier l'information non IT.

- Quid de l'ISO 27002 ?
 - D'une certaine façon, certains points de l'ISO 27002 sont phagocytés par ITIL
 - Ce n'est pas grave, puisque l'ISO 27002 n'est qu'un guide de bonnes pratiques
 - Restent les mesures de sécurité ne concernant pas l'IT
- Voies de recherche
 - Tableau de correspondance
 - ITIL → ISO 27001 (clauses + annexe A)
 - ISO 27001 (clauses + annexe A) → ITIL
 - Documents d'application
 - Pour chaque point de l'ISO, sélection dans ITIL de ce qui est nécessaire

- Merci

Alexandre Fernandez-Toro
Alexandre.Fernandez@hsc.fr