

# ITIL & ISO2700x

Club - 27001- Toulouse

- ❖ Sébastien Rabaud
- ❖ Michel Viala



## ❖ Intervenants

- Michel VIALA : Consultant ITIL confronté à la prise en compte des aspects sécurité (exigences issues de politiques sécurité, de projet ISO2700x) dans les processus ITIL
- Sébastien RABAUD : Consultant Sécurité confronté à la mise en œuvre de mesures sécurité ISO27001 en environnement ITIL

## ❖ Contexte - Démarche

- Mise en commun des expertises et retours d'expériences
- Identification des synergies
- Définition d'une approche commune ITIL/ISO2700x

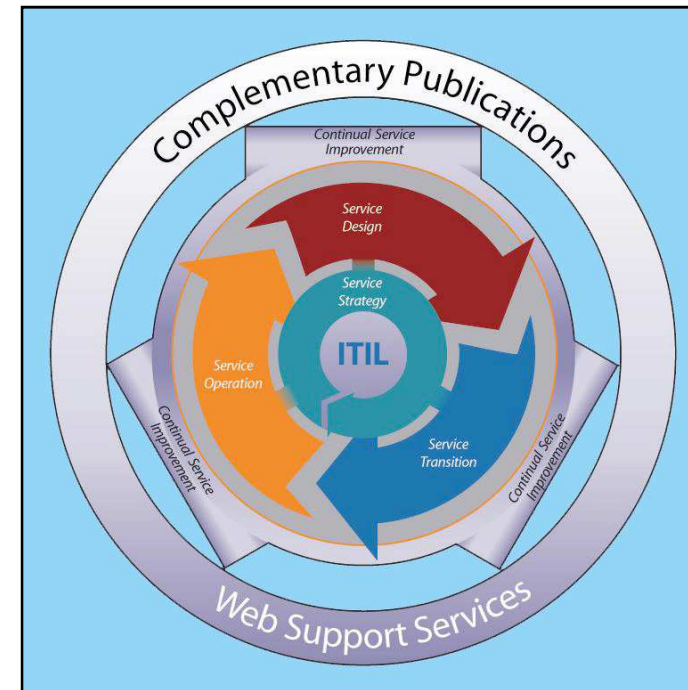
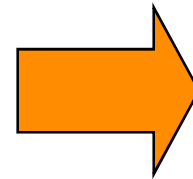
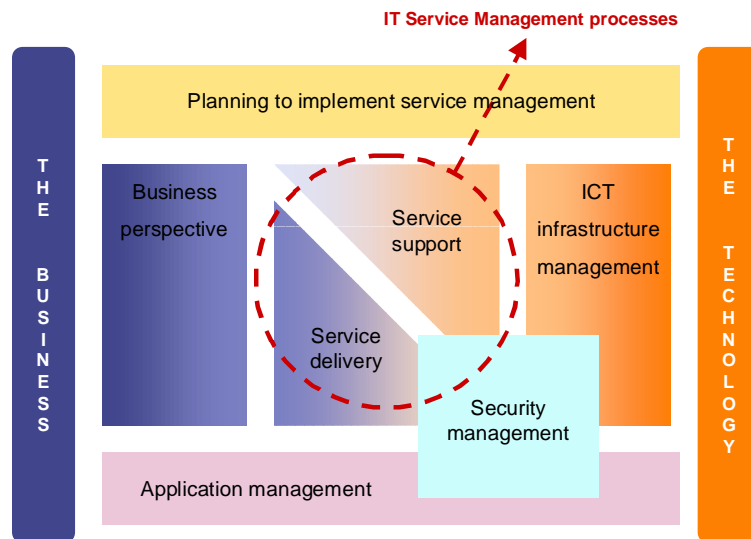


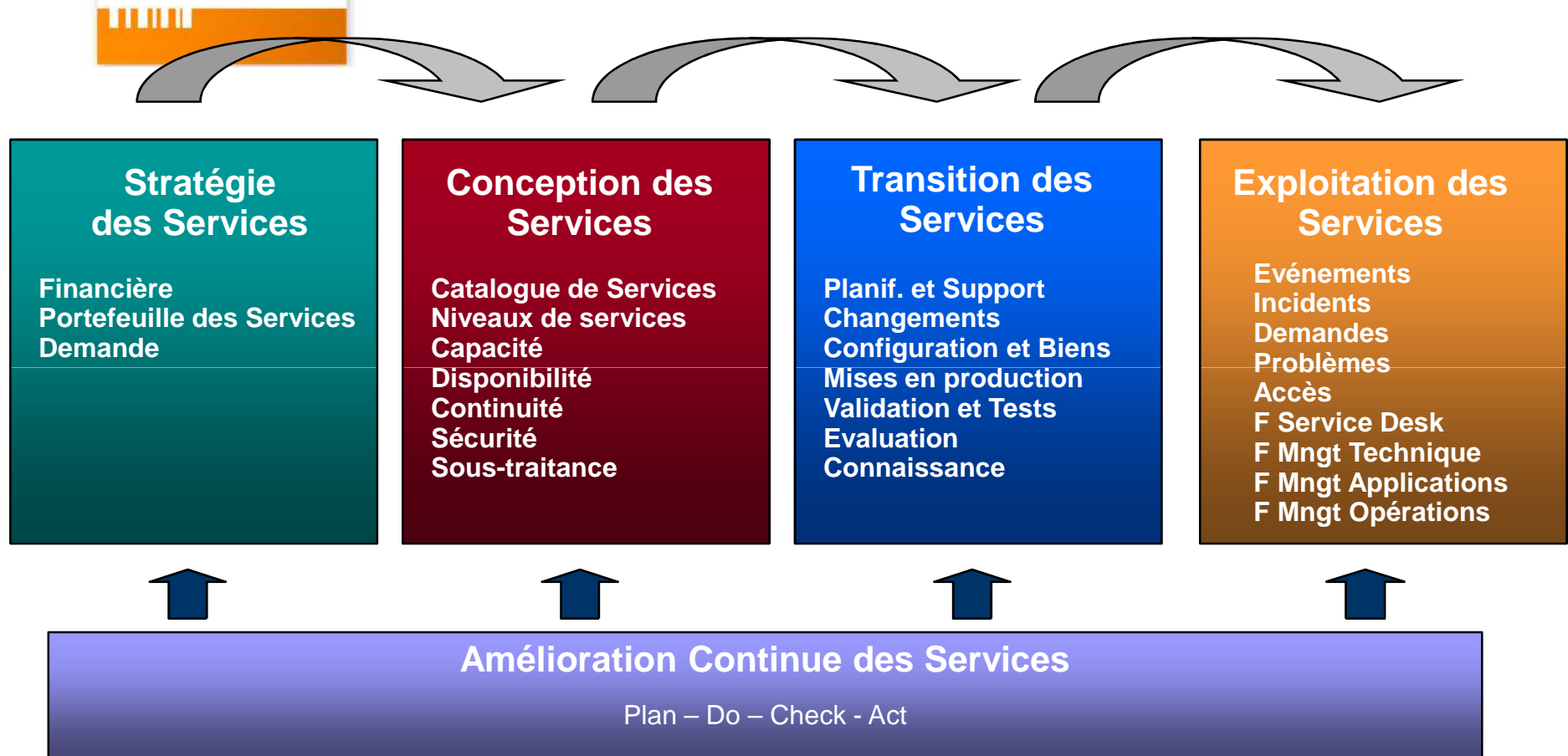
- ❖ Positionnement ITIL
  
- ❖ « Synergies » ITIL & ISO 2700x
  - La gestion de la sécurité dans ITIL ... et les normes ISO 2700x
  - Utiliser ITIL pour mettre en œuvre ISO 27001 ?
  
- ❖ Retour d'expériences – Etude de cas
  - Gestion des incidents liés à la sécurité de l'information



- ❏ Référentiel de bonnes pratiques en matières de fourniture de services informatiques aux Métiers
  
- ❏ Cycle de vie des Services
  - Stratégie / Conception / Transition / Exploitation
  - Amélioration Continue des Services : PDCA
  
- ❏ Approche Processus
  - et fonctions (Service Desk, ...)







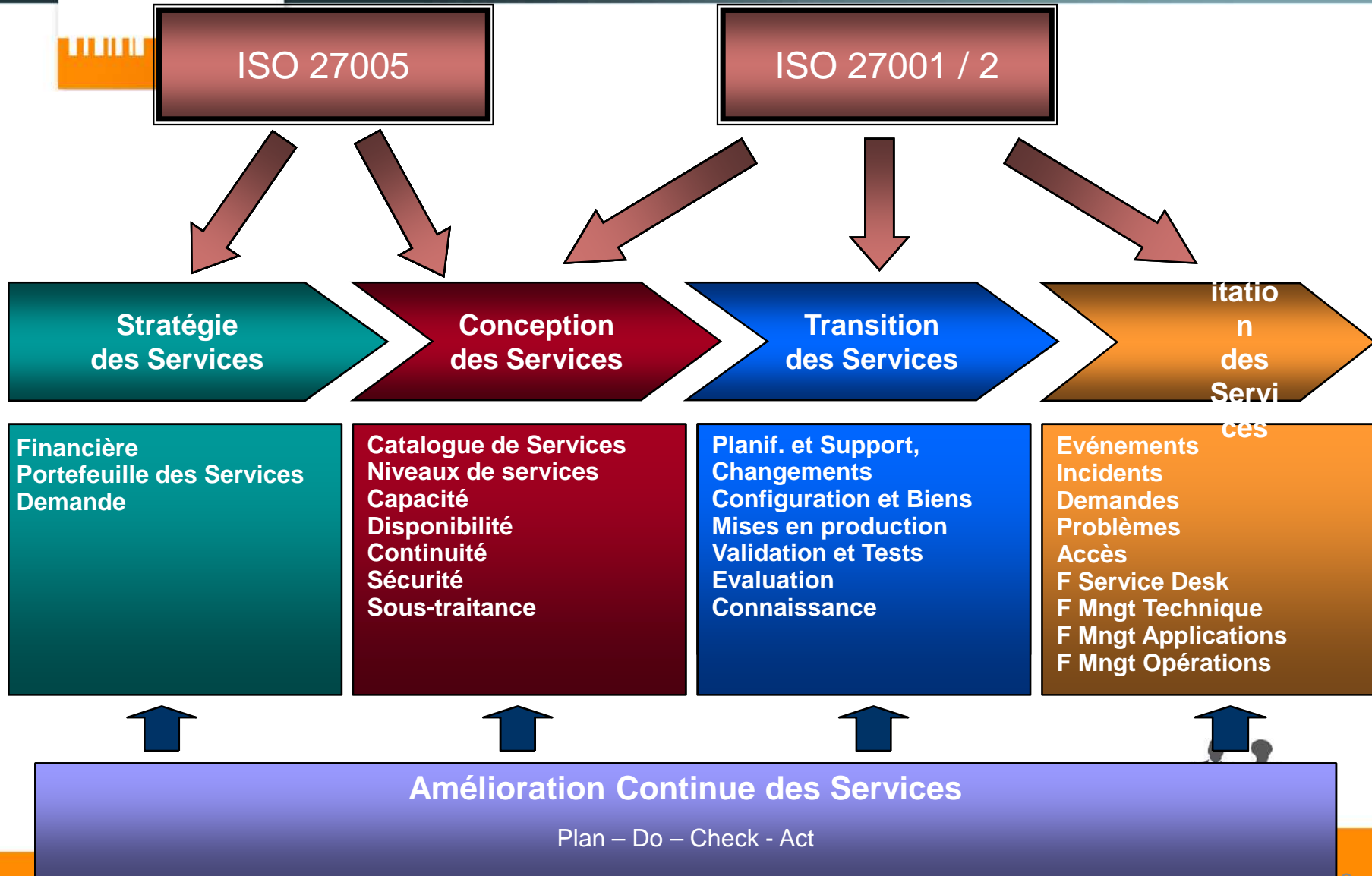
- ❖ Les objectifs du processus ISM sont :
  - D'une part d'aligner la sécurité de l'information avec la sécurité métier
  - D'autre part d'assurer que la sécurité de l'information est gérée effectivement dans toutes les activités de Gestion des Services.
  
- ❖ La gestion de la sécurité dans ITIL fait référence à ISO2700x
  - => Appliquer ISO27001



- ❖ ISO27005 = Comment gérer les risques ?
  
- ❖ ISO27002
  - Objectifs et mesures de sécurité
  - **Préconisations de mise en œuvre**
  
- ❖ ISO27001 = SMSI
  - Gérer les risques => ISO27005 (ou autres)
  - Sélectionner les objectifs et mesures de sécurité
  - **Mettre en œuvre / implémenter les mesures de sécurité**
  - Surveiller/réexaminer, mettre à jour/améliorer ... et ainsi de suite ...



# Interfaces entre ISO 2700x et ITIL



## ❖ Mettre en œuvre / implémenter des mesures de sécurité ISO27001 (conformément aux préconisations ISO27002) à l'aide d'ITIL

- Pour chaque mesure de sécurité :
  - Identifier les différents processus ITIL sur lesquels s'appuyer
- Pour chaque processus ITIL identifié :
  - Prendre en compte les besoins associées à chaque mesure de sécurité
  - ... et les préconisations ISO27002 associées



## ✕ Processus ITIL sur lesquels ISO 2700x peut s'appuyer (\*) :

<b>A.7.1 Responsabilités relatives aux actifs</b>		
<i>Objectif</i> : Mettre en place et maintenir une protection appropriée des actifs de l'organisme.		
Inventaire des actifs	<i>Mesure</i> Tous les actifs doivent être clairement identifiés et un inventaire de tous les actifs importants doit être réalisé et géré	Gestion des configurations
Propriété des actifs	<i>Mesure</i> La propriété de chaque information et des moyens de traitement de l'information doit être 'attribuée' <sup>3</sup> , à une partie définie de l'organisme.	Gestion des configurations
Utilisation correcte des actifs	<i>Mesure</i> Des règles permettant l'utilisation correcte de l'information et des actifs associés aux moyens de traitement de l'information doivent être identifiées, documentées et mises en œuvre.	

<b>A.10.1 Procédures et responsabilités liées à l'exploitation</b>		
<i>Objectif</i> : Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.		
A.10.1.1	Procédures d'exploitation documentées	<i>Mesure</i> Les procédures d'exploitation doivent être documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.
A.10.1.2	Management des modifications	<i>Mesure</i> Les changements apportés aux systèmes et moyens de traitement de l'information doivent être contrôlés.
A.10.1.3	Séparation des tâches	<i>Mesure</i> Les tâches et les domaines de responsabilité doivent être séparés pour réduire les occasions de modification ou de mauvais usage non autorisé(e) ou involontaire des actifs de l'organisme.
A.10.1.4	Séparation des équipements de développement, d'essai et d'exploitation	<i>Mesure</i> Les équipements de développement, d'essai et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans le système d'information en exploitation.

(\*) et compléter lorsque nécessaire



# Gestion des incidents liés à la sécurité de l'information



## ❖ Objectifs et mesures ISO27001

- A.13.1 : « ... mode de notification ... permet ... action corrective, dans les meilleurs délais »
  - Remontée / Signalement des événements sécurité (A.13.1.1/.2)
- A.13.2 : « ... Approche cohérente et efficace ... »
  - « ... responsabilité, procédures ... réponse rapide, efficace et pertinente » (A.13.2.1)
  - « ... mécanismes ... quantifier, surveiller ... volume, coûts » (A.13.2.2)

## ❖ Préconisations ISO27002

- Procédures formelles, responsable désigné, utilisateurs informés
- Mécanismes simples et connus de tous
- Responsabilités et procédures, amélioration continue : surveillance, évaluation, correction



## ❖ Gestion des incidents

- « Quantifier », « volume » (A.13.2.2) => Identifier les incidents liés à la sécurité
- Evaluer les impacts
  - A posteriori <= « couts » (A.13.2.2)
  - À priori <= « réponse pertinente » (A.13.2.1) => gestion des niveaux de service (expression de besoins)

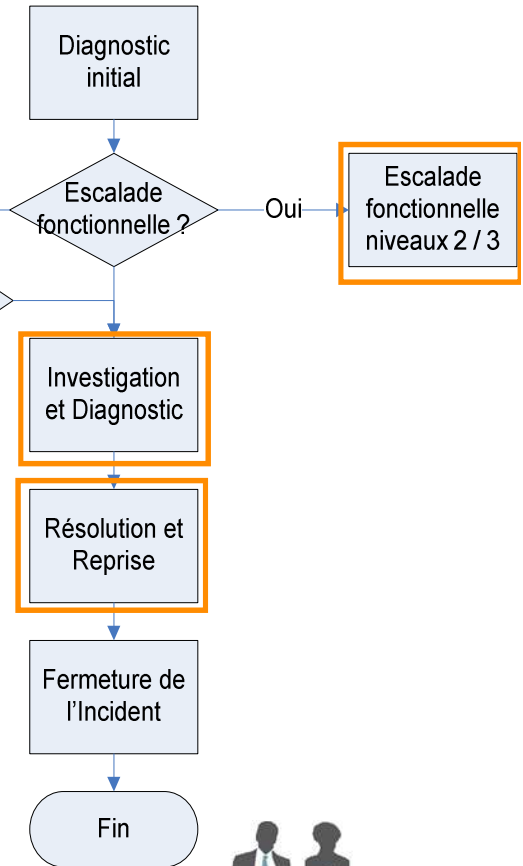
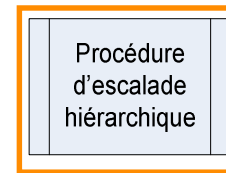
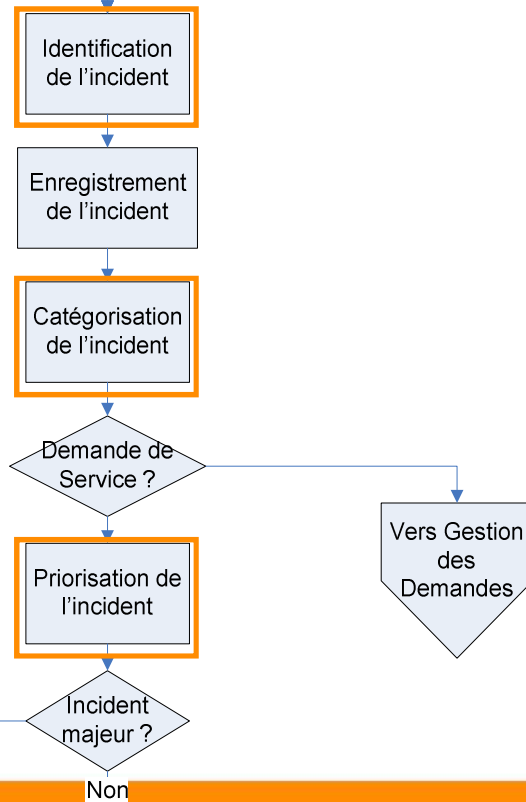
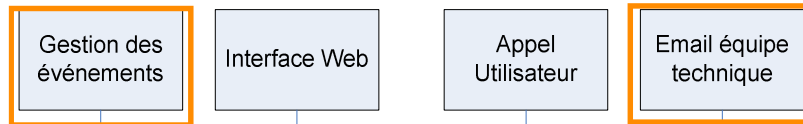
## ❖ Gestion des évènements

- « Signaler » (A.13.1.1) => Détecter les evts de sécurité
- « voies hiérarchiques appropriés » => Circuit de remontée
- « Garantir ... meilleurs délais » => « automatisation »



ISO 27001 / 2

## Exigences



## 📌 Points clés

- Définition ISO27000 d'un évènement et d'un incident lié à la sécurité de l'information à « affiner » / « instancier »
  - Alerte = Incident (« ... présentant un probabilité ... de ... »)
  - Critères de classification
    - Origine : Anomalie/Accident, Erreur, Malveillance
    - Impacts (besoins) DICA
    - Autres : non respects politiques de sécurité, baisse niveau sécu
  - Liste des types d'évènements et d'incidents sécurité
    - Métiers : immobiliers (infos sur les acquisitions foncières), public (délibération élus), e-commerce (phishing)



## 📌 Points clés

- « mini démarche » de gestion des risques pour chaque incident (« réponse pertinente », )
  - => Évaluation / Décision / Traitement
- Evaluation des impacts (« réponse pertinente », « coûts »)
  - Intégration des critères sécurité (IC notamment) dans les « règles de priorisation » des incidents ITIL ...
  - Intégration dans les procédures (« à priori », « à posteriori »)
- Rôles et responsabilités en matière de sécurité (ISO27001), Communication / Sensibilisation



- ITIL permet d'implémenter les mesures ISO27001 sur son périmètre
- Niveau d'implémentation d'ITIL (complétude et maturité) = Indice d'efficacité et de « facilité » à répondre aux besoins ISO27001



## ❖ La suite ...

- Gestion des vulnérabilités techniques (A.12.6.1 ≈ A.13.2.1)
  - Gestion des correctifs => changement, MEP, ...
  - Gestion vulnérabilités => incidents, événements
- Gestion des niveaux de service ↔ ISO27005
  - Expression des besoins de sécurité => ISO27005
  - Prise en compte des besoins de sécurité => ITIL – Gestion des niveaux de service
- Identifier les domaines pour lesquels ITIL n'apporte pas de support



What else ? 😊  
(Questions)

Merci de votre attention



# Annexes



# ITIL : Interfaces ISM avec processus ITIL (1)

- ❖ **Gestion des Incidents et des Problèmes** fournissent assistance pour la résolution et la correction des incidents et problèmes sécurité. Le processus de Gestion des Incidents doit permettre d'identifier et de gérer les incidents sécurité. Les équipes Service Desk et Opérations doivent « reconnaître » les incidents sécurité.
- ❖ **Gestion de la Continuité de Service** : avec l'estimation des impacts et risques Métier. Un plan ITSCM est une exigence (obligatoire) de ISO 27001.,
- ❖ **Gestion des Niveaux de Service** : avec la détermination de besoins sécurité et des responsabilités et leur introduction dans les SLR et SLA; l'investigation et la résolution de failles sécurité sur les services et les composants.
- ❖ **Gestion des Changements** : avec pour chacun des changements, l'évaluation de l'impact sur la sécurité et les contrôles sécurité. ISM peut aussi donner des informations sur les changements non autorisés.
- ❖ Des question sur la législation et les Ressources Humaines peuvent être levées lors d'investigations sécurité.



# ITIL : Interfaces ISM avec processus ITIL (2)

- ❖ **Gestion des Configurations** fournit des informations précises pour aider à la classification sécurité. Un système de gestion de configuration efficace est une entrée efficace de ISM.
- ❖ Sécurité est souvent considérée comme un élément de **Gestion de la Disponibilité**, puisque Confidentialité, Intégrité et Disponibilité sont l'essence de Gestion de la Disponibilité et d'ISM. De même, ISM devrait travailler avec Gestion de la Disponibilité et Gestion de la Continuité pour conduire les activités de d'Analyse des Risques.
- ❖ **Gestion des Capacités** doit prendre en compte les implications sécurité lors de la sélection et l'introduction de nouvelles technologies.
- ❖ **Gestion Financière** devrait fournir les fonds adéquats pour finances les besoins en sécurité.
- ❖ **Gestion des Fournisseurs** avec l'inclusion dans les contrats concernant les responsabilités des fournisseurs, des termes et conditions, et des conditions d'accès aux services et systèmes.



## ✕ Processus ITIL sur lesquels ISO 2700x peut s'appuyer (\*) :

<b>A.7.1 Responsabilités relatives aux actifs</b>		
<i>Objectif</i> : Mettre en place et maintenir une protection appropriée des actifs de l'organisme.		
Inventaire des actifs	<i>Mesure</i> Tous les actifs doivent être clairement identifiés et un inventaire de tous les actifs importants doit être réalisé et géré	Gestion des configurations
Propriété des actifs	<i>Mesure</i> La propriété de chaque information et des moyens de traitement de l'information doit être 'attribuée' <sup>3</sup> , à une partie définie de l'organisme.	Gestion des configurations
Utilisation correcte des actifs	<i>Mesure</i> Des règles permettant l'utilisation correcte de l'information et des actifs associés aux moyens de traitement de l'information doivent être identifiées, documentées et mises en œuvre.	

<b>A.10.1 Procédures et responsabilités liées à l'exploitation</b>		
<i>Objectif</i> : Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.		
A.10.1.1	Procédures d'exploitation documentées	<i>Mesure</i> Les procédures d'exploitation doivent être documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.
A.10.1.2	Management des modifications	<i>Mesure</i> Les changements apportés aux systèmes et moyens de traitement de l'information doivent être contrôlés.
A.10.1.3	Séparation des tâches	<i>Mesure</i> Les tâches et les domaines de responsabilité doivent être séparés pour réduire les occasions de modification ou de mauvais usage non autorisé(e) ou involontaire des actifs de l'organisme.
A.10.1.4	Séparation des équipements de développement, d'essai et d'exploitation	<i>Mesure</i> Les équipements de développement, d'essai et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans le système d'information en exploitation.

(\*) et compléter lorsque nécessaire



## ✕ Processus ITIL sur lesquels ISO 2700x peut s'appuyer (\*) :

<b>A.10.2 Gestion de la prestation de service conclus avec un tiers</b>			
<i>Objectif</i> : Mettre en œuvre et maintenir un niveau de sécurité de l'information et de service adéquat et conforme aux accords de prestation de service conclus avec un tiers.			
A.10.2.1	Prestation de service	<i>Mesure</i> Il doit être assuré que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers.	Gestion des sous-traitants
A.10.2.2	Surveillance et examen des services tiers	<i>Mesure</i> Les services, rapports et enregistrements fournis par les tiers doivent être régulièrement contrôlés et réexaminés, et des audits doivent être régulièrement réalisés.	Gestion des sous-traitants
A.10.2.3	Gestion des modifications dans les services tiers	<i>Mesure</i> Les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte de la criticité des systèmes et processus de gestion concernés et de la réévaluation du risque.	Gestion des changements ( ? )

<b>A.11.2 Gestion des accès des utilisateurs</b>			
<i>Objectif</i> Contrôler l'accès des utilisateurs autorisés et empêcher les accès non autorisés aux systèmes d'information.			
A.11.2.1	Enregistrement des utilisateurs	<i>Mesure</i> Une procédure formelle d'inscription et désinscription des utilisateurs destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information doit être définie.	Gestion des accès
A.11.2.2	Gestion des privilèges	<i>Mesure</i> L'attribution et l'utilisation des privilèges doivent être restreintes et contrôlées.	Gestion des accès
A.11.2.3	Gestion du mot de passe utilisateur	<i>Mesure</i> L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.	Gestion des accès
A.11.2.4	Réexamen des droits d'accès utilisateurs	<i>Mesure</i> La direction doit réexaminer les droits d'accès utilisateurs à intervalles réguliers par le biais d'un processus formel	Gestion des accès

(\*) et compléter lorsque nécessaire



## ✕ Processus ITIL sur lesquels ISO 2700x peut s'appuyer (\*) :

<b>A.13 Gestion des incidents liés à la sécurité de l'information</b>			
<b>A.13.1 Remontée des événements et des failles liés à la sécurité de l'information</b>			
<i>Objectif</i> Garantir que le mode de notification des événements et failles liés à la sécurité de l'information permet la mise en œuvre d'une action corrective, dans les meilleurs délais.			
A.13.1.1	Remontée des événements liés à la sécurité de l'information	<i>Mesure</i> Les événements liés à la sécurité de l'information doivent être signalés, dans les meilleurs délais, par les voies hiérarchiques appropriées.	Gestion des événements Gestion des incidents
A.13.1.2	Remontée des failles de sécurité	<i>Mesure</i> Il doit être demandé à tous les salariés, contractants et utilisateurs tiers des systèmes et services d'information de noter et de signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.	Gestion des événements Gestion des incidents
<b>A.14 Gestion de la continuité de l'activité</b>			
<b>A.14.1 Gestion de la continuité de l'activité d'un point de vue aspects de la sécurité de l'information</b>			
<i>Objectif</i> : Empêcher les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets causés par les défaillances majeures des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.			
A.14.1.1	Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité	<i>Mesure</i> Un processus de continuité de l'activité dans l'ensemble de l'organisme doit être élaboré et géré, qui satisfait aux exigences en matière de sécurité de l'information requises pour la continuité de l'activité de l'organisme.	Gestion de la continuité de service
A.14.1.2	Continuité de l'activité et appréciation du risque	<i>Mesure</i> Les événements pouvant être à l'origine d'interruptions des processus métier doivent être identifiés, tout comme la probabilité et l'impact de telles interruptions et leurs conséquences pour la sécurité de l'information.	Gestion de la continuité de service
A.14.1.3	Élaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	<i>Mesure</i> Des plans doivent être élaborés et mis en œuvre pour maintenir ou restaurer l'exploitation et assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.	Gestion de la continuité de service
A.14.1.4	Cadre de la planification de la continuité de l'activité	<i>Mesure</i> Un cadre unique pour les plans de continuité de l'activité doit être géré afin de garantir la cohérence de l'ensemble des plans, de satisfaire de manière constante aux exigences en matière de sécurité de l'information et d'identifier les priorités en matière de mise à l'essai et de maintenance.	Gestion de la continuité de service
A.14.1.5	Mise à l'essai, gestion et réévaluation constante des plans de continuité de l'activité	<i>Mesure</i> Les plans de continuité de l'activité doivent être testés et mis à jour régulièrement afin de s'assurer qu'ils sont actualisés et efficaces.	Gestion de la continuité de service

(\*) et compléter lorsque nécessaire



Fin de la présentation

