École sur les bonnes pratiques organisationnelles pour les Administrateurs Système et Réseaux (ASR)
CISP Paris - 15 au 18 octobre 2019

Organisation de la SSI

O. Brand-Foissac

Plan

- Objectif
- Démarche de mise en place
- Amélioration continue (PDCA)
- Les étapes concrètes de mise en place
- Appréciation des risques

Objectif

- La norme ISO27001 constitue le référentiel pour la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI)
  - L'ISO27002 est un outil de sélection des mesures de sécurité à mettre en œuvre dans un processus SMSI
- Objectif du SMSI : assurer une confiance dans les systèmes d'information

Démarche de mise en place

- Cinématique (phase Plan) :
  - Périmètre du SMSI
  - Politique du SMSI
  - Plan de gestion des Risques
    - Appréciation des risques
    - Identification et évaluation des risques
    - Traitement des risques
  - Objectifs de sécurité
  - Déclaration d'applicabilité

Définition du périmètre du SMSI

- Définition des besoins et objectifs de l'unité
- Identification des processus métier

- Définir les exigences de sécurité
- Exclusions

Définition de la politique du SMSI

- Préciser les objectifs de sécurité
- Prends en compte la réglementation

  exigences LRC (légales, réglementaires et contractuelles)
- Prends en compte la gestion de risque

Plan de gestion des risques

- Définir l'approche d'appréciation du risque
  - Méthodologie d'appréciation
  - Définition des critères d'acceptation
  - Identifier les niveaux de risque acceptables

    (ISO27005 gestion du risque)

Objectifs de sécurité (1)

- Objectifs et mesures de sécurité
  - Selon les résultats de l'appréciation des risques
  - Depuis ISO27001:Annexe A et ISO27002
    - Aucune mesure n'est obligatoire (quoique)
    - Permet de ne rien oublier
    - Possibilité de prendre d'autres mesures que celles proposées

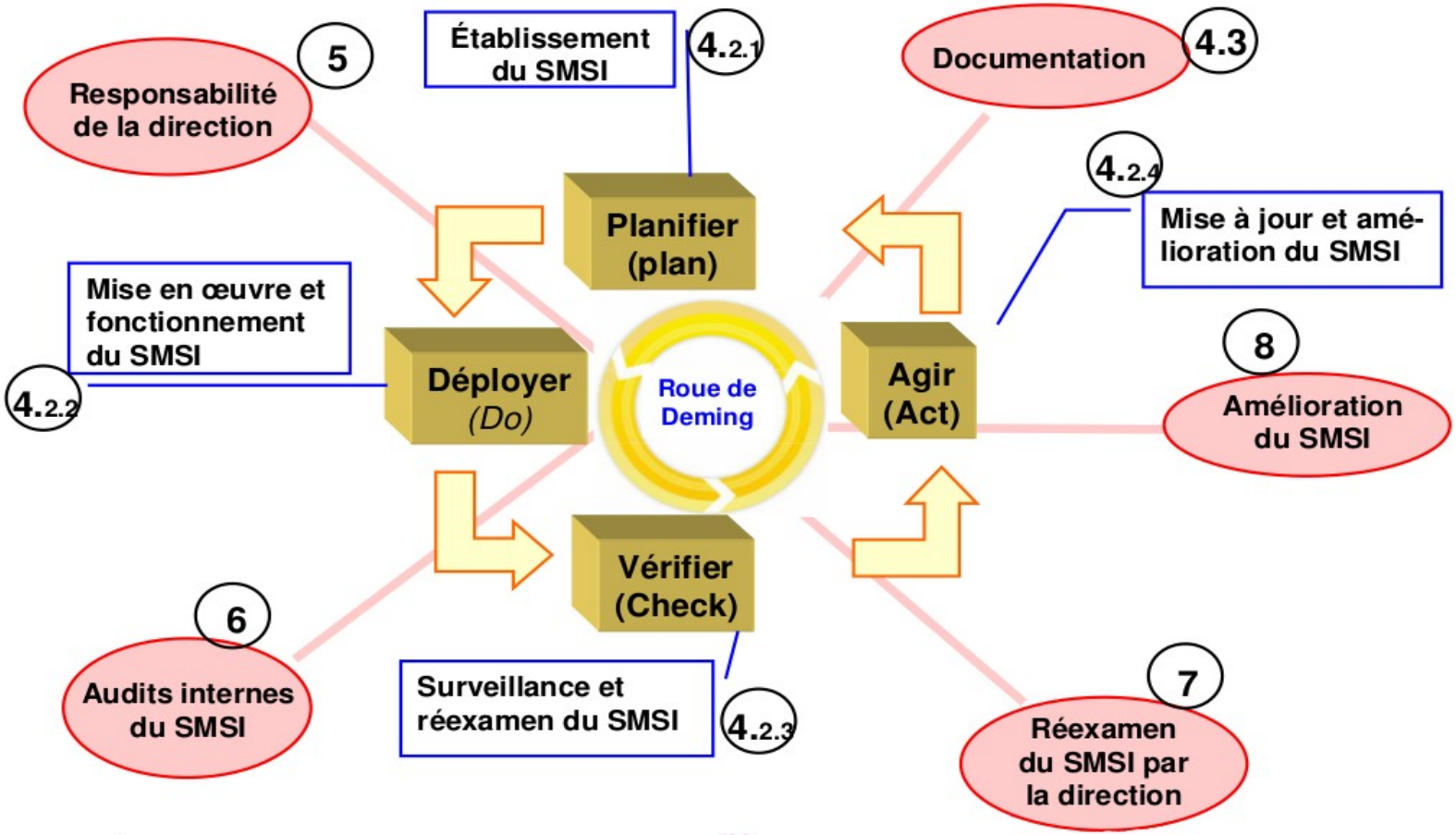
Objectifs de sécurité (2)

- Risques résiduels
  - Obtenir l'approbation de la direction
    - Identification
    - Possible lien avec le catalogue de services
- Obtenir l'autorisation de la direction
  - Mettre en œuvre le SMSI
  - Exploiter le SMSI

Déclaration d'applicabilité (DdA)

- Ce document contient
  - Objectifs de sécurité
  - Mesures de sécurité retenues
    - Et les raisons de leur sélection
  - Mesures mises en place
  - Mesures non retenues
    - Et les raisons de leur mise à l'écart
- Permet de ne rien oublier

Amélioration continue



(Réf. aux chapitres de ISO27001-2005)

PDCA : Planifier

- (P) *Plan* : planifier
  - - sélection du périmètre
    - Doit intégrer les actifs primordiaux
    - Si possible les actifs de soutien
  - Ne pas choisir dès le début un périmètre trop important
  - Commencer par un état de l'existant
    - … et des mesures actuellement en place

PDCA : Déployer

- (D) *Do* : déployer
  - Choisir des faits
    - mesurables
  - Choisir des indicateurs
    - Pertinents, fiables
    - Uniquement sur ce qui est mis en place dans le SMSI (permet de connaitre : l'application et l'efficacité des mesures de protection)
  - Tableau de bord
    - Pilotage
    - Pas trop d'indicateurs (idéalement 3 à 5)

PDCA : Contrôler

- (C) *Check* : contrôler (au sens de surveiller)
  - Vérification régulière des indicateurs
  - Réaction aux incidents
  - Noter les possibilité d'amélioration (pour la phase Agir)
  - Suivi

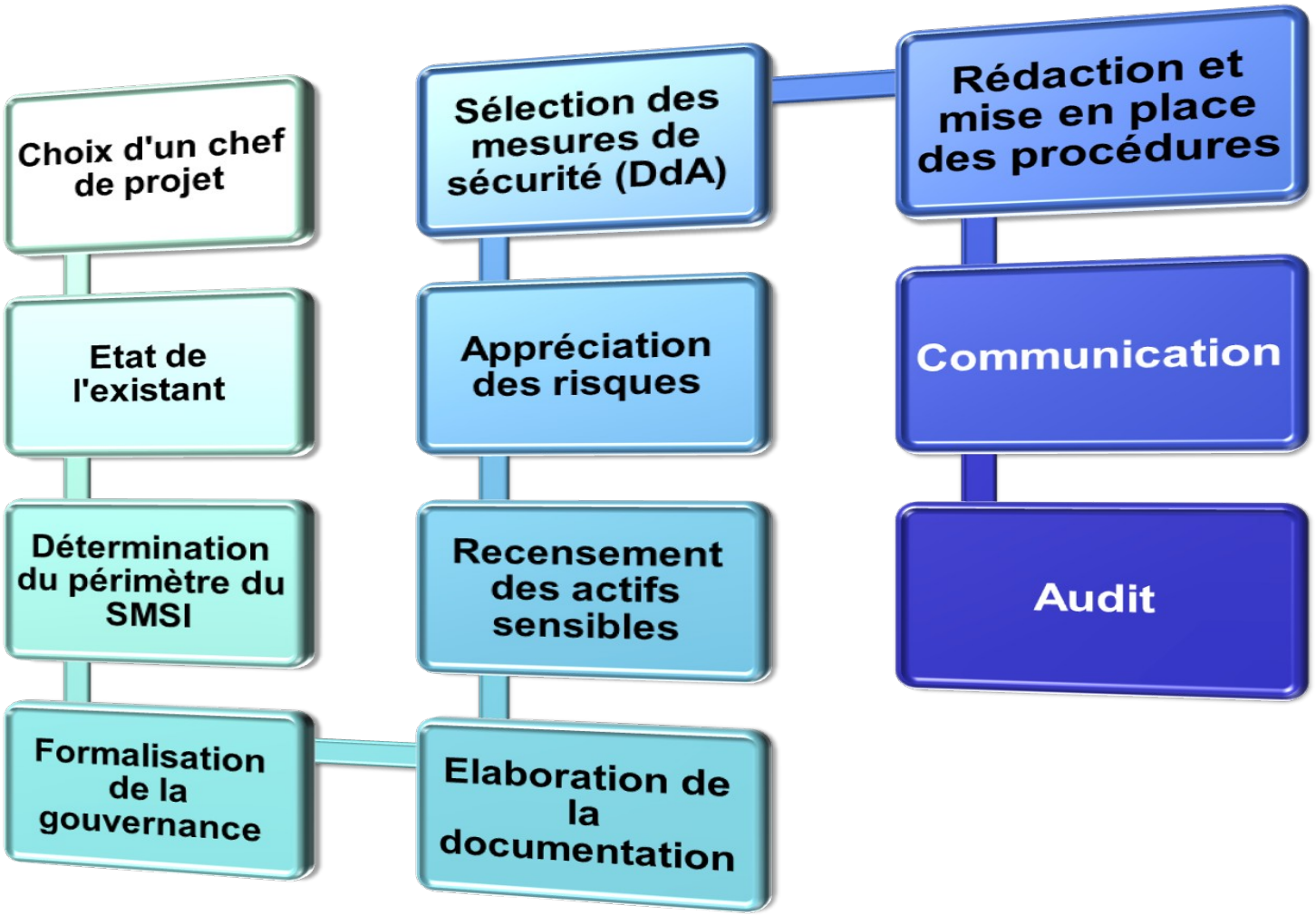
PDCA : Agir

- (A) *Act* : agir, mettre-à-jour et améliorer
  - Correction du système (écarts entre souhaité et réalisé)
  - Intégration de nouveaux actifs
    - Augmentation du périmètre
    - Ajout/suppression dans le périmètre
  - Prépare la planification de l'étape suivante

    (Plan de la boucle suivante)
  - Rapport, documentation

Les étapes concrètes de mise en place

Les étapes de mise en place



Les étapes de mise en place

- Lancement de la procédure par le DU
  - Démarrage officiel (date)
  - Constitution d'un comité
    - Sert à recenser les besoins, à contrôler les adéquations, à pré-valider les étapes
    - Veille à faire circuler les informations concernant la sécurité (sensibilisation des utilisateurs,...)
  - Implication de la direction
    - (respect des engagements, sensibilisation ...)

Etape : Identification des actifs

- La définition du périmètre d'application du SMSI passe par l'identification et la localisation des actifs (primordiaux et de soutien)
  - ils doivent être identifiés et classés par risques (voir appréciation des risques)
- Le périmètre est constitué de la liste des actifs/processus qui sont pris en charge dans le SMSI et de ceux écartés du domaine

Etape : Appréciation des risques

- Définir la politique d'appréciation des risques pour le domaine concerné par le SMSI (approuvée par la direction)
- Identifier les risques
- Analyser et évaluer les risques
- Choisir le traitement des risques
  - Voir le Guide des Bonnes Pratiques, Ch.3

Etape : Sélection des mesures de sécurité

- Le choix des mesures de sécurité à mettre en place, dépend :
  - Du niveau de risque souhaité
  - Du coût de mise en place vis-à-vis de la valeur des actifs
  - Des ressources nécessaires (astreintes,temps homme)
  - l'ISO27002-2005/2013 regroupe les 133 critères en 39 objectifs de sécurité

    Permet d'établir la Déclaration d'Applicabilité (DdA)

Etape : rédaction des procédures

- Documenter les procédures
  - Plan de continuité d'activité
  - Plan de reprise d'activité
  - Plan de gestion des incidents
- Mise en œuvre du système de mesures (génération des indicateurs)
- Mise en place des tableaux de bord
- ...

Appréciation du risque

Références

- ISO27005 : Guide de mise en œuvre de la partie appréciation des risques de ISO27001 (entre dans la gestion de risque en général ISO31000)
  - Analyse de risque
    - Identification et estimation des risques
  - Evaluation des risques
    - Etablit priorité et ordonnancement des risques
- Suivie du traitement et acceptation des risques

Vocabulaire

- Risque = ?
  - danger (ingénieur)
  - événement (modéliste)
  - incertitude par rapport aux objectifs (manager)
  - menace, fondamentalement négatif (santé)
  - rendement (finance)
  - interruption de service (secteur public)

Vocabulaire

- Risque = ?
  - danger (ingénieur)
  - événement (modéliste)
  - incertitude par rapport aux objectifs (manager)
  - menace, fondamentalement négatif (santé)
  - rendement (finance)
  - interruption de service (secteur public)

Réf. ISO-31000

Définition du risque

- Conjonction de 3 critères
  - Vulnérabilité, faiblesse
  - Menace, probabilité d'exploitation de la vulnérabilité
  - Impact, conséquences

Analyse de risque

- L'identification et estimation du risque
  - Impact
    - Quelles sont les actifs à protéger ?
    - Quelle est leur importance (valeur) ?
  - Vulnérabilité
    - Quels sont les moyens d'accéder/modifier ces actifs ? Quelles sont leurs protections ?
  - Menace
    - Quelle est la probabilité qu'une personne, un processus exploite cette vulnérabilité ?
      - Faille connue disponible sur internet, ...

Traitement des risques (1)

- Refusé
  - Le risque est trop élevé, pas de mesure de sécurité réaliste pour le réduire, l'activité est supprimée
- Transféré
  - vers un sous-traitant qui saura mieux le gérer
- Réduit
  - Application de mesures de sécurité
  - Risque résiduel
- Accepté : prise de risque

Traitement des risques (2)

- Dans cette étape
  - Intégrer les coûts notamment dans le choix des mesures de sécurité
    - Coût du transfert
    - Coût de mise en œuvre de la réduction du risque
    - Coût de réalisation de la menace (prise de risque)

Traitement du risque (3)

- La direction doit accepter les risques résiduels
  - Donc le plan de traitement du risque dans sa globalité
  - Implique une documentation formelle
  - Si des contraintes de budget ou de temps ne permettent pas de déployer les mesures, la responsabilité de la direction est engagée (pas celle du responsable SSI)

Exemple

- Localiser les risques
  - Y compris sur les défenses périmétriques