Les processus d'un SMSI

Modèle de SMSI et retours d'expérience

Julien Levrard
<Julien.Levrard@hsc.fr>

Besoin d'un modèle générique

- Uniformisation des démarches dans les SMSI qu'HSC accompagne
- Capitalisation des expériences sur les prestations SMSI
- Obtention d'un modèle générique, compréhensible par un profane comme une direction
- Découpage logique des activités d'un SMSI

Démarche d'analyse

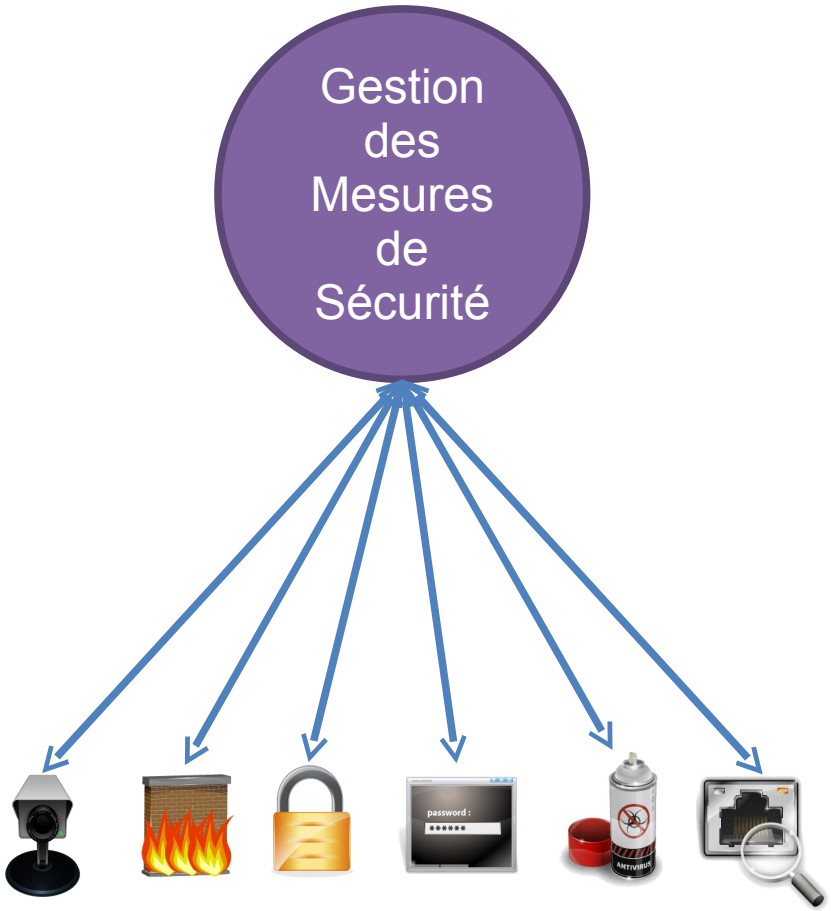
- Réfléchir aux questions légitimes d'une direction...
- … et des postulats de base du management de la sécurité...
- … avec la norme ouverte à proximité

Mesures de sécurité

- Postulat 1 :

  Aucune organisation n'a attendu la publication d'une norme ISO pour mettre en œuvre des mesures de sécurité.

Gestion des mesures de sécurité

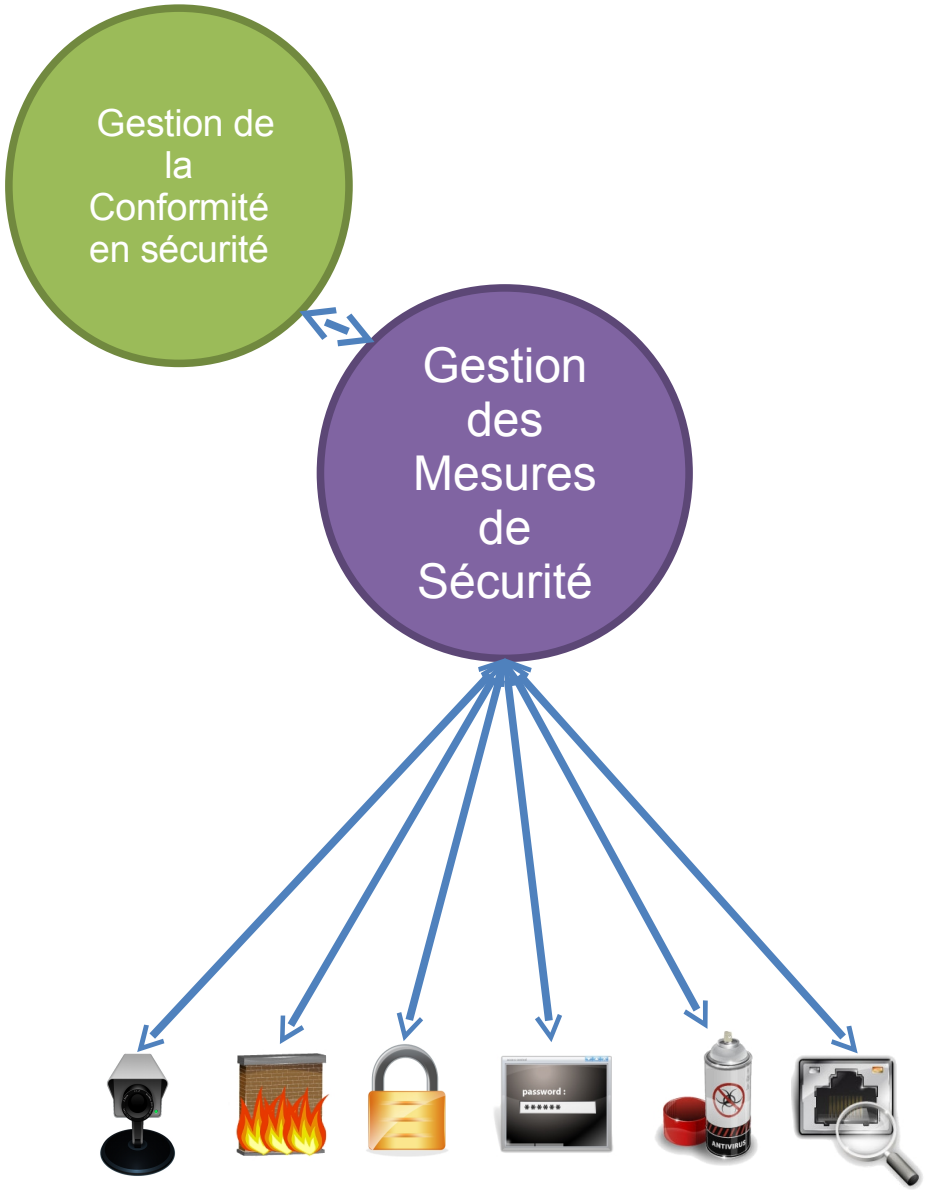


- Sait-on :
  - Quelles mesures de sécurité sont mises en œuvre ou en projet ?
  - Quelles activités sont associées à ces mesures et qui les réalise ?

- Postulat 2 :

  Le minimum attendu d'un RSSI est qu'il ait une réponse à ces questions.

Gestion de la conformité

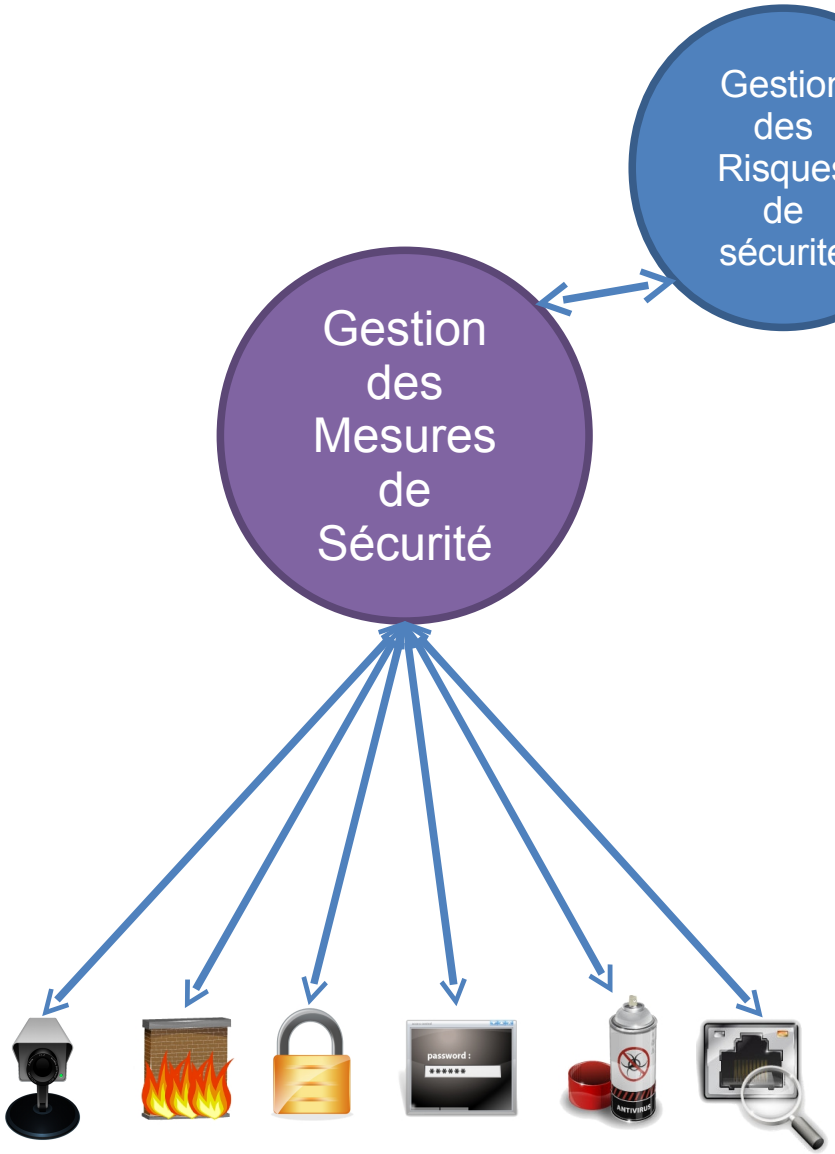


- Le RSSI a-t-il identifié
  - Les obligations légales, règlementaires et contractuelles applicables en termes de sécurité ?
  - Les mesures à mettre en œuvre pour les respecter ?

- Postulat 3 :

  Le RSSI de l'organisation connaît les obligations légales, règlementaires et contractuelles en sécurité et fait ce qu'il faut pour nous éviter les tourments judiciaires et la prison.

Gestion des risques



- Le RSSI a-t-il identifié/compris
  - Les attentes de mes parties prenantes ?
  - Les informations et processus importants à protéger ?
- Les budgets alloués à la sécurité sont-ils utilisés à bon escient ?
- Le RSSI a-t-il une bonne compréhension du SI qui lui permet d'anticiper les incidents ?

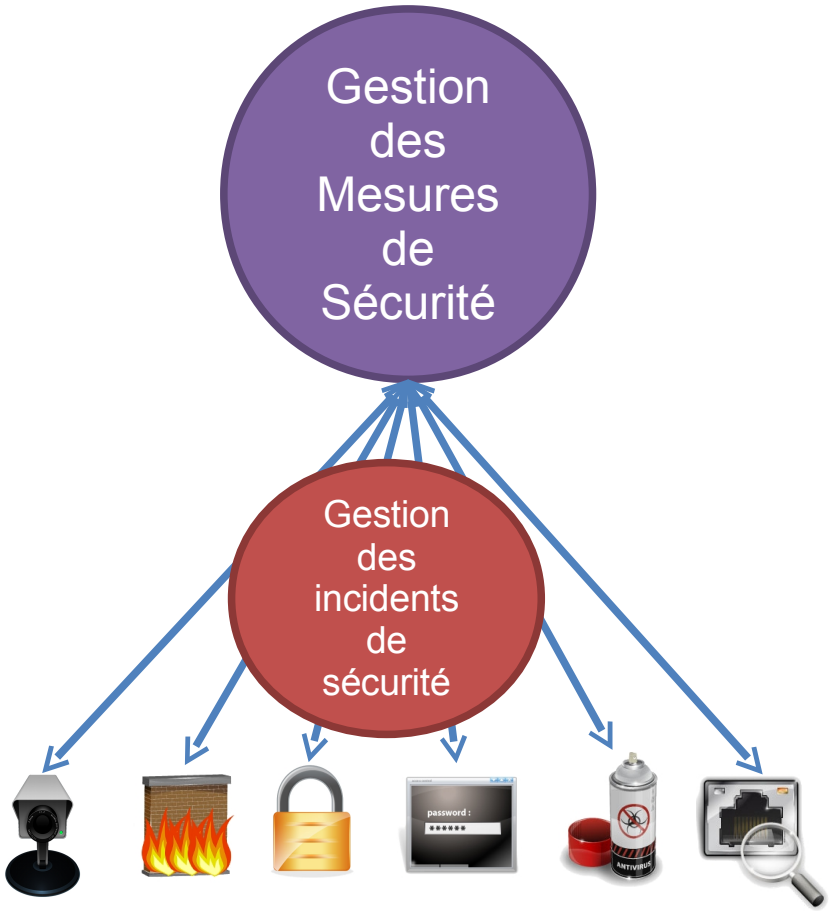
- Postulat 4 :

Le RSSI comprend les risques métiers, sait les interpréter en termes SI et adapte les dépenses pour réduire ces risques en priorité

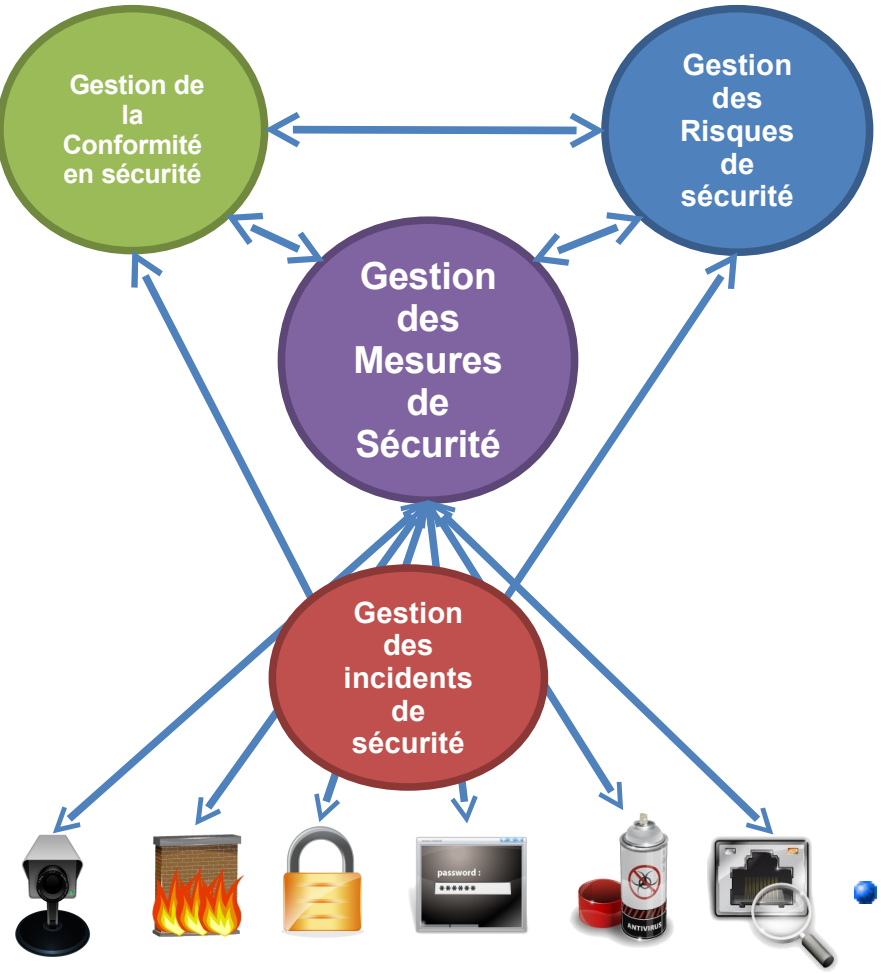
Gestion des incidents

- Postulat 5 :

  Si un incident grave lié à la sécurité de l'information, est mal géré, le RSSI peut être renvoyé.

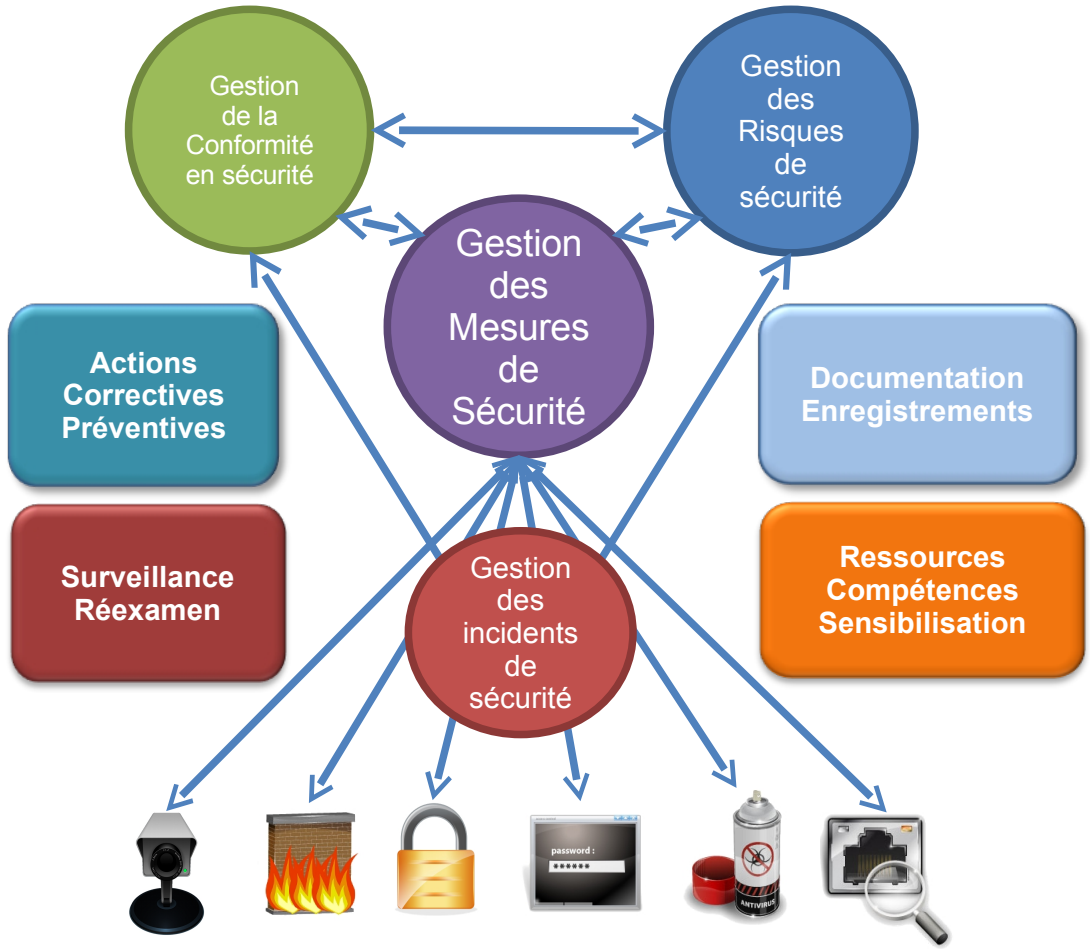


Récapitulatif



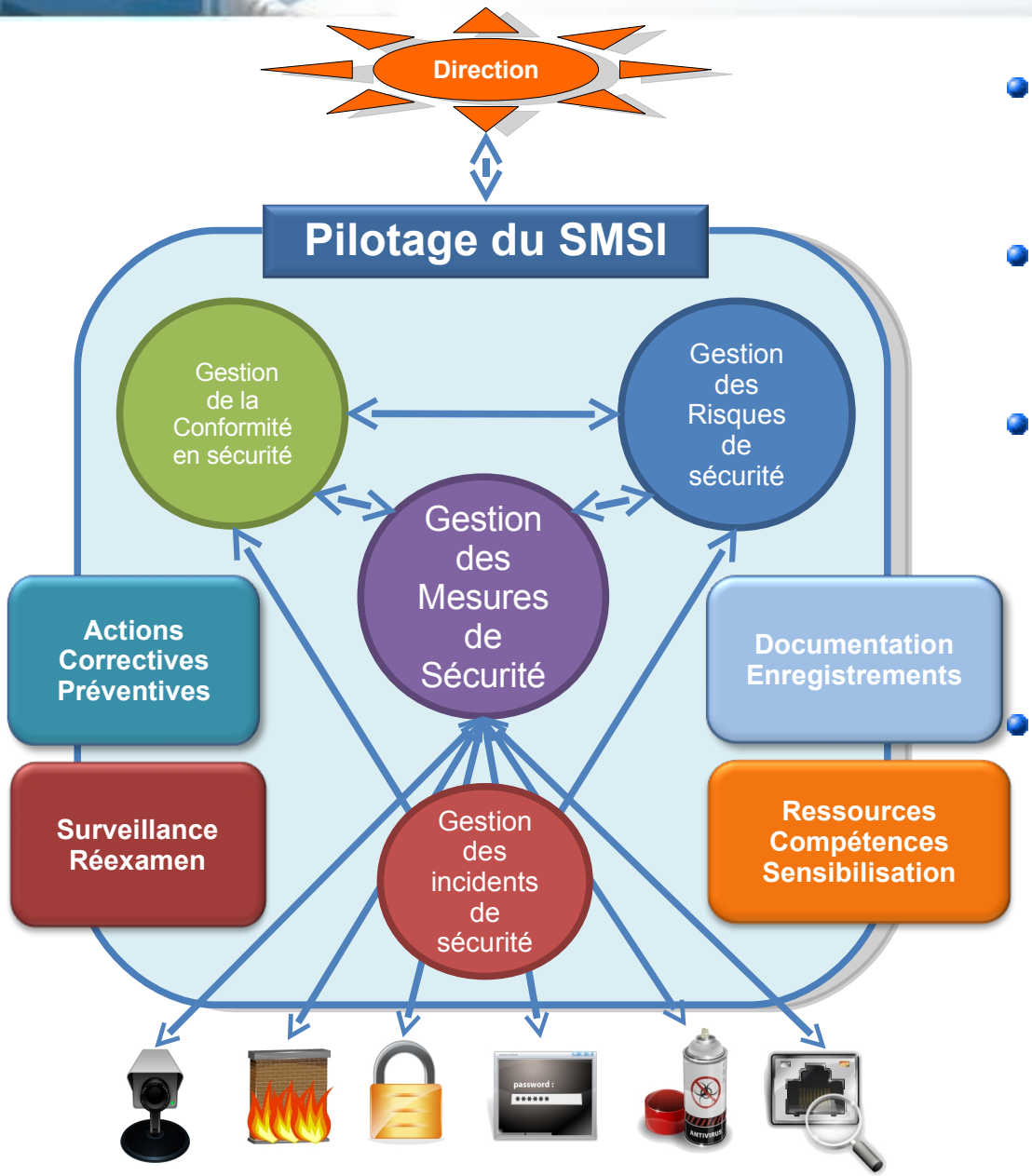
- 5 postulats :
  - Aucune organisation n'a attendu une norme ISO pour mettre en œuvre des mesures de sécurité
  - Le RSSI sait quelles mesures de sécurité sont en place ou en projet et qui est responsable des activités associées
  - Le RSSI connaît les obligations légales, règlementaires et contractuelles et initie les actions appropriées
  - Le RSSI comprend les risques métiers, sait les interpréter en termes SI et adapte les investissements pour réduire ces risques en priorité
  - Un incident grave mal géré peut faire renvoyer le RSSI
- **N'importe quelle organisation qui prétend gérer sa sécurité du SI peut se reconnaître dans ce modèle**

Système de management de la sécurité de l'information



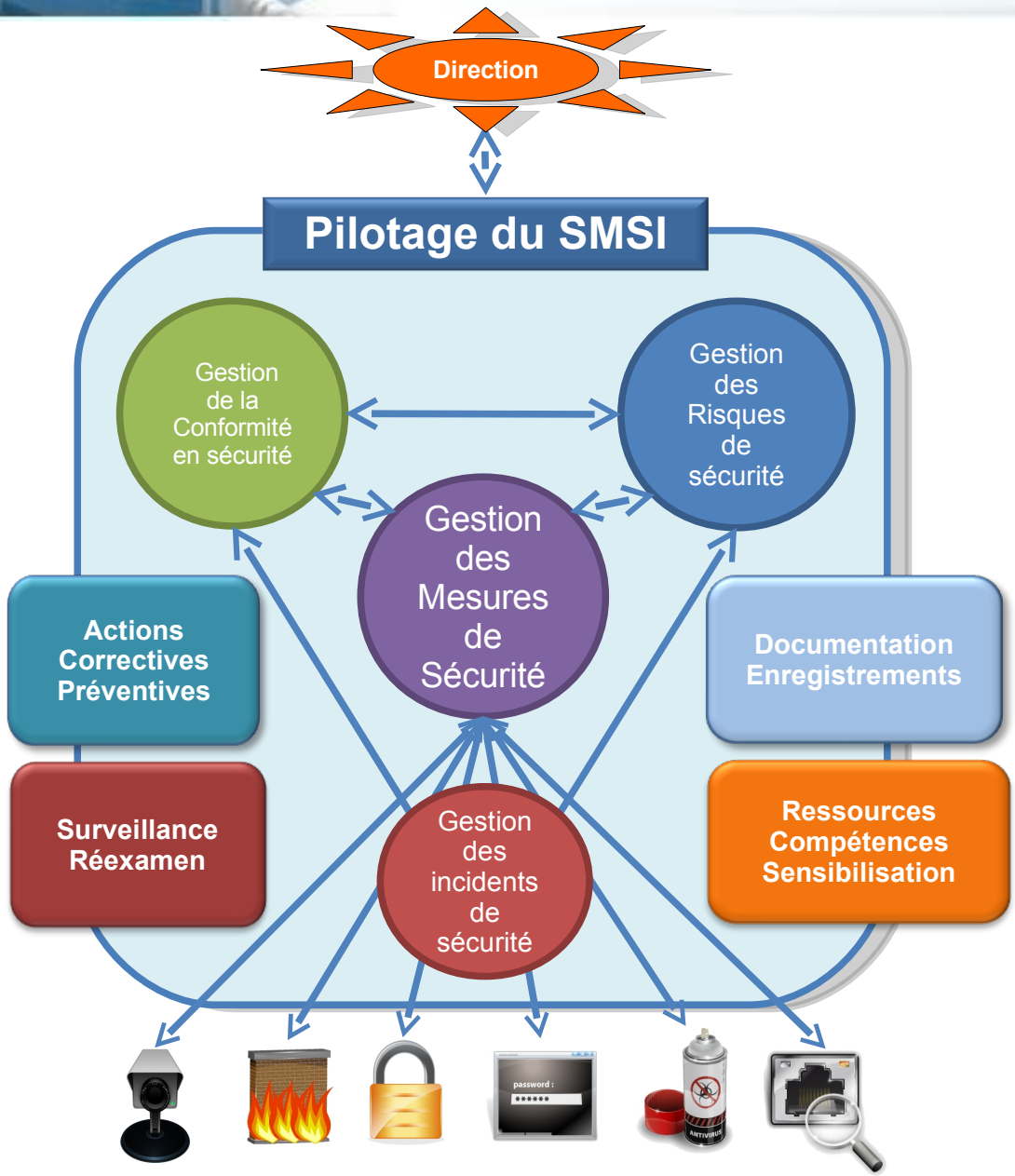
- Application du PDCA sur les mesures de sécurité et les processus de gestion
  - Gestion de la documentation
  - Gestion des enregistrements
  - Gestion des ressources
  - Gestion des compétences
  - Surveillance et réexamen
  - Gestion des actions correctives et préventives

SMSI conforme à la norme ISO 27001



- Impliquer formellement la direction
- Formaliser l'organisation de la sécurité
- Distinguer les activités de construction du SMSI (projet) et d'exploitation du SMSI (processus)
- Formaliser les documents obligatoires du SMSI
  - Politique du SMSI
  - Plan de traitement des risques
  - Déclaration d'applicabilité
  - Etc.

Intérêt du modèle proposé



- Schématise le processus idéal de gestion de la sécurité
- Applicable à toute organisation (comme la norme)
- Simple à expliquer à des non-experts
- Découpe le SMSI en blocs logiques
  - Évaluation de la maturité facile
  - Plans d'action structurés et clairs
  - Justifie certaines mesures de sécurité de la DdA
- Utilisable comme référentiel
  - De diagnostic
  - D'accompagnement
  - D'audit interne

Quelques retours d'expérience

Retour d'expérience

- Erreur : Gérer les clauses de la norme une par une séquentiellement
  - Projet de conformité
  - Alimentation d'un outil de gestion de la conformité par des clauses de l'ISO 27001

- Solution : Utiliser un modèle de processus de SMSI éprouvé
  - En l'adaptant à son contexte et à sa conception de la gestion de la sécurité

Retour d'expérience

- Erreur : Gérer le SMSI uniquement en mode projet
  - La norme mélange dans ses clauses :
    - **La cible** : Une sécurité du SI gérée à l'état de l'art (cf. modèle)
    - Les **étapes du projet** pour atteindre la cible
- Erreur : Ne pas nommer de RSSI
  - Nommer un chef de projet SMSI (chargé de mission)
- Solution : Anticiper le mode processus dès le projet
  - Gestion des actions projet → Gestion des Actions Correctives et préventives
  - Entretiens de l'identification des risques → Audit interne des mesures de sécurité
  - Comité de pilotage → comité sécurité
  - Chef de projet → RSSI

Retour d'expérience

- Erreur : Considérer les 133 mesures de l'annexe A pour réduire les risques
  - Quels risques ne sont pas réduits par
    - A.5.1.1, A.6.1.1, A.8.2.2, A.15.1.1 ?
  - Comment ne pas les sélectionner ?
  - A l'inverse, comment mesurer la réduction d'un risque précis par ces mesures ?

- Solution : intégrer les mesures de sécurité concernées dans les processus de gestion du SMSI
  - Le plan de traitement des risques devient plus technique (mesures A.9, A.10, A.11 et A.12)
  - Plus lisible et plus concret pour les opérationnels

Retour d'expérience

- Erreur : Ne pas impliquer les opérationnels pour la gestion des mesures de sécurité
  - Documentation, surveillance
  - Lien faible entre le RSSI et les opérationnels
  - Management intermédiaire
  - Toujours plus rapide et plus facile de documenter des mesures de sécurité par le RSSI ou des consultants
  - Entraîne un SMSI qui ne vit pas, voire une double documentation

- Solution : Encadrer, expliquer, supporter, vérifier, revoir, sensibiliser mais surtout ne pas « faire à la place »
- Solution : Impliquer le management intermédiaire comme relais d'action

Retour d'expérience

- Erreur : Utiliser la Déclaration d'Applicabilité comme outil de suivi des mesures de sécurité
  - A moins d'apprécier le classement de l'annexe A...
  - Rend la communication et le travail sur les mesures de sécurité extrêmement pénible et laborieux
- Erreur : Considérer la DdA comme un Plan de traitement des risques

- Solution : Grouper les mesures par thème/responsable/actif et n'utiliser la DdA que comme un outil de communication avec l'auditeur et les parties prenantes
- Solution : Considérer un PTR « maîtrise d'ouvrage » géré par le RSSI et plusieurs PTR « maîtrise d'œuvre » : DSI, RH, RSSI, etc.

Retour d'expérience

- Erreur : Choisir un micro-périmètre
  - La plupart des processus et des mesures de sécurité est gérée par des tiers
  - L'atteinte des objectifs est principalement liée à la bonne définition et à la formalisation des clauses contractuelles avec les tiers
  - Un SMSI conforme à l'ISO-27001 est vide de sens dans ce contexte, les contrats et les audits des tiers suffisent à rassurer les parties prenantes

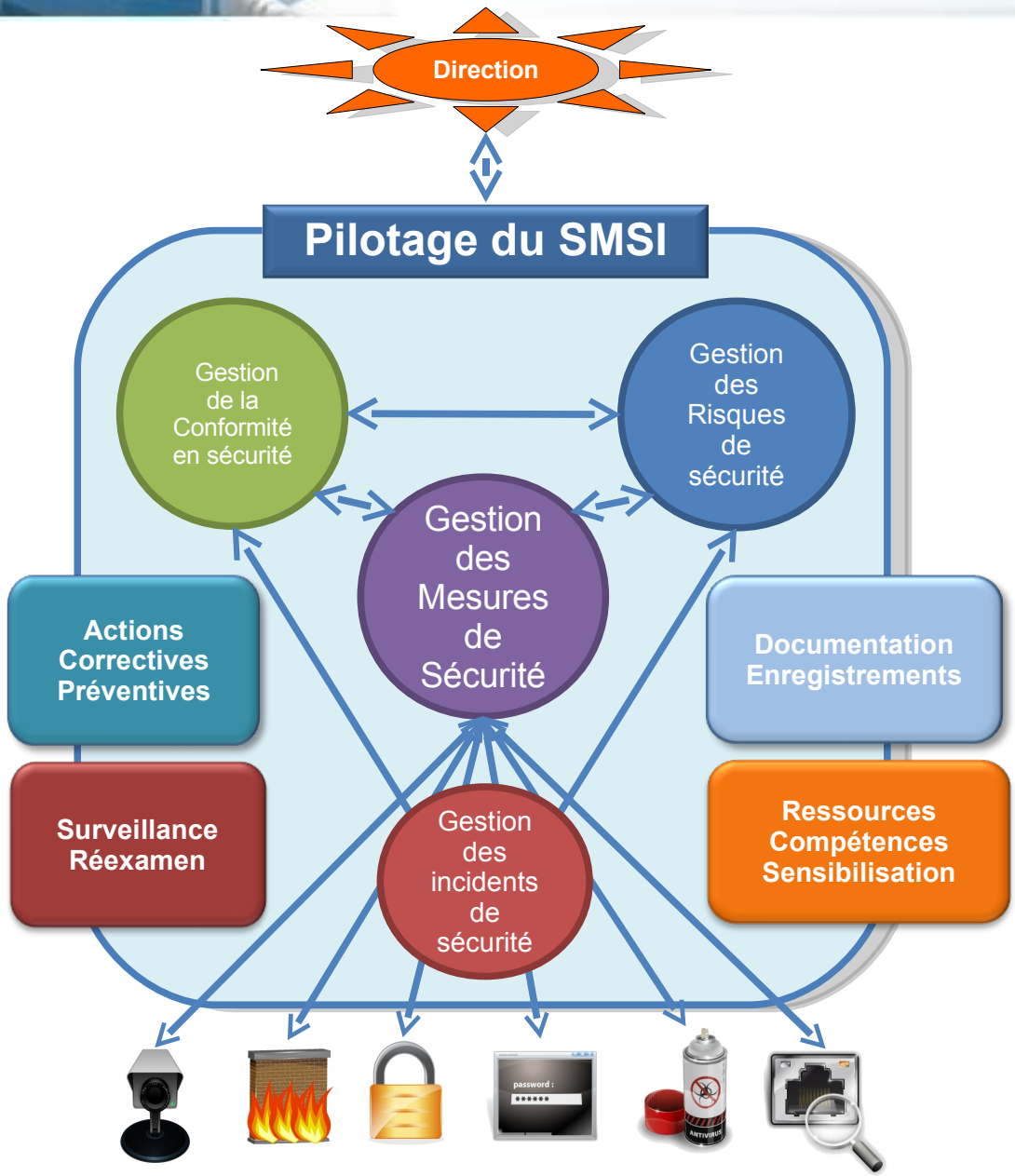
- Solution : ne considérer la mise en place d'un SMSI que sur un périmètre sur lequel on réalise concrètement de la gestion de la sécurité

Retour d'expérience

- Erreur : Ne pas développer la surveillance et le réexamen
  - Incapacité du RSSI à valider les mesures mises en œuvre
  - Sous-estimation du coût de l'audit interne et de la production d'enregistrement
  - Enfermement dans l'aspect théorique du SMSI
  - SMSI à sens unique

- Solution : investir fortement dans l'évaluation des mesures de sécurité et dans l’interaction avec les opérationnels dès le début du projet.

Sujets en cours de développement



- Prise en compte des retours des consultants pour adapter le modèle
- Définition d'ateliers de gestion des mesures de sécurité par thème
- Optimisation des SMSI et de nos prestations
- Intégration de référentiels complémentaires
  - SMSI multi-référentiels (Données de santé, CNIL, PCI-DSS)
- Recherche d'indicateurs pertinents

Questions ?

?