« Politiques de Sécurité de l'Information »

Club 27001

Toulouse – 12 Avril 2013

Sébastien RABAUD – SCASSI Conseil
sebastien.rabaud@scassi.com

Politiques de sécurité
Sommaire

- « Politiques » et « sécurité »
- Constats
- Besoins et objectifs des politiques de sécurité
- Structure / Contenu des politiques de sécurité
- Mise en œuvre des politiques de sécurité

« Politiques » et « Sécurité »

- Les politiques dans un organisme
  - Exemples :
    - Ressources humaines, Achats / Fournisseurs, Commerciale, Qualité produit, …
  - Définition :
    - Stratégie, lignes directrices, règles de fonctionnement, …
    - Liées à un processus, une activité, …
    - Documenté … ou pas

- Les politiques de sécurité
  - Exemples :
    - Industrielle, des personnes, des bâtiments, …
    - **De l'Information, des Systèmes d'Information, du SMSI**

Politiques de sécurité
Constats

- Un unique document monolithique … « copier / coller » de ISO27002 (« LA PSI »)
- Un magma de documents hétérogènes :
  - notes de services, mails, chartes, procédures opérationnelles, …
- Rien du tout …
- Pas mis à jour, « poussiéreux », …
- Inutilisés car …
  - Pas ou peu connu des acteurs pertinents
  - Inutilisable
    - Pas assez précis / applicable pour certains acteurs (administrateurs systèmes, réseaux, chef de projet, …)
    - Trop précis pour d'autres (Chefs de projet, managers, …)
- Niveau d'application / de conformité inconnu !

Politiques de sécurité
Pourquoi ?

Quels sont les besoins et objectifs ?

- Une politique de sécurité de l'information pour répondre à des exigences

  - **Clients :**
    - avec référentiel (« Maison », 27001)
    - … ou sans => « Qu'attends l'auditeur ? »

  - **RGS**

2.2.4 - Élaborer une politique SSI

Il est recommandé d'élaborer et de formaliser une politique SSI globale au niveau de l'AA. Selon les besoins, cette politique SSI pourra être déclinée et complétée notamment pour un domaine particulier, ou pour un système d'information précis.

Le guide [PSSI] fournit une aide pour élaborer une politique SSI.

Politiques de sécurité
Pourquoi ?

- Quels sont les besoins et objectifs ?
  - Une politique de sécurité de l'information pour répondre à des <u>exigences</u>

    - **PCI-DSS**

Conditions PCI DSS
12.1 Définir, publier, gérer et diffuser une politique de sécurité qui remplit les fonctions suivantes :
12.1.1 Satisfait toutes les exigences de la norme PCI DSS.
12.1.2 Inclut un processus annuel qui identifie les menaces et les vulnérabilités, et débouche sur une évaluation formelle des risques.
12.1.3 Comprend au moins un examen annuel et est mise à jour chaque fois que l'environnement change.
12.2 Élaborer des procédures de sécurité opérationnelles quotidiennes conformes aux exigences de cette spécification (par exemple, des procédures de gestion des comptes d'utilisateur et des procédures d'examen des journaux).

Politiques de sécurité
Pourquoi ?

Quels sont les besoins et objectifs ?

- Une politique de sécurité de l'information pour répondre à des <u>exigences</u>

  - **27001 : Etablissement du SMSI**

b) définir une politique pour le SMSI en termes de caractéristiques de l'activité, de l'organisme, de son emplacement, de ses actifs, et de sa technologie, qui:

1) inclut un cadre pour fixer les objectifs et indiquer une orientation générale et des principes d'action concernant la sécurité de l'information;

2) tient compte des exigences liées à l'activité et des exigences légales ou réglementaires, ainsi que des obligations de sécurité contractuelles;

3) s'aligne sur le contexte de management du risque stratégique auquel est exposé l'organisme, dans lequel se dérouleront l'établissement et la mise à jour du SMSI;

4) établit les critères d'évaluation future du risque [voir 4.2.1c)];

5) a été approuvée par la direction.

NOTE Pour les besoins du présent document, les politiques relatives au SMSI sont considérées comme un surensemble de la politique relative à la sécurité de l'information. Ces politiques peuvent être décrites dans un seul document.

Politiques de sécurité
Pourquoi ?

Quels sont les besoins et objectifs ?

- Une politique de sécurité de l'information pour répondre à des exigences

  - **27001 : Annexe A**

A.5 Politique de sécurité		
A.5.1 Politique de sécurité de l'information *Objectif:* Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.		
A.5.1.1	Document de politique de sécurité de l'information	*Mesure* Un document de politique de sécurité de l'information doit être approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.

Politiques de sécurité
Pourquoi ?

- Quels sont les besoins et objectifs ?

  - Une politique de sécurité de l'information pour répondre à un besoin, une thématique précise
    - BYOD, réseaux sociaux, …

  - Une politique de sécurité de l'information pour :
    - définir, communiquer, partager les règles de sécurité
    - … auprès des bons interlocuteurs avec le bon niveau de détails
    - concernant tout ou partie des domaines de la sécurité de l'information
    - s'adapter aux évolutions
      - Des risques
      - De l'organisation
    - plutôt une cible à atteindre qu'un recueil de ce que l'on est capable de faire

Politiques de sécurité
Structure

Structure multi-niveaux

Niveau	Objet	Contenu, Exemples
1	Stratégie, Général	Principes généraux : Fonction SSI, Rôles et responsabilités SSI
2	Thématiques	Domaines SSI : Contrôle d'accès, Traces, Tiers, …
3	Détaillées	Réseau, Systèmes, Application n
4	Guides, Procédures SSI	S'appliquant à plusieurs processus / services
Autres	Transverses / « périphériques »	Chartes, Note d'organisation, Politique de sécurité applicable aux fournisseurs

Politiques de sécurité
Structure

Structure multi-niveaux

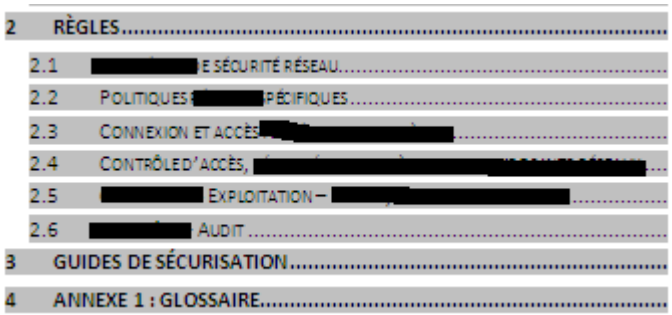
- Les politiques thématiques (N2)
  - regroupent l'ensemble des règles d'une thématique s'appliquant à l'ensemble de l'organisme
  - sont utilisables / applicables directement en tant que référentiel
  - peuvent être utilisés pour définir une politique de niveau 3
  - *Exemples : Contrôle d'accès logique, Gestion des traces, alertes, incidents, …*

Profils d'habilitations
Responsable fonctionnel
Gestionnaire technique
Utilisateur
Responsable [redacted]

Politiques de sécurité
Structure

Structure multi-niveaux

- Les politiques détaillées (N3)
  - regroupent les règles d'un « domaine » pour l'ensemble des thématiques (« héritage » du niveau 2),
  - permet à certains acteurs d'avoir un seul document référent
  - permet d'instancier, de préciser, d'ajouter certaines règles
  - *Exemples : Réseau, Système, Bureautique, Application RH, …*



Profils d'habilitations	Responsabilités	Fonction
Responsable [redacted]	Responsable de la gestion des habilitations [redacted] s réseaux [redacted] .) concernant un exploitant [redacted] doit être validée [redacted] par ce responsable.	[redacted]
Gestionnaire [redacted]	Personnel en charge [redacted], chacune d'elle devant obligatoirement faire l'objet d'une validation par le responsable fonctionnel	[redacted]

Politiques de sécurité
Structure

Structure multi-niveaux

- *Les guides et procédures SSI (N4)*
  - Ne sont pas des politiques mais répondent à des besoins de guides ou procédures « génériques » :
    - Soit pour répondre à des besoins transverses particuliers. *Ex : procédure de déclaration CNIL (à l'usage des responsables de traitement)*
    - Soit pour faciliter l'élaboration, l'amélioration de procédures opérationnelles. *Ex : procédure de création d'accès utilisateur*

Politiques de sécurité
Structure

Structure multi-niveaux

- *Les documents « autres, transverses »*
  - Ne sont pas des politiques mais répondent à des besoins particuliers
    - *Chartes : d'usage du système d'information, éditoriale, …*
    - *Politiques de sécurité applicables par les tiers*
    - Documents de sensibilisation : *supports de présentation, …*
    - Communications ponctuelles : *alertes, notes, …*
    - Matrice de correspondance entre un référentiel imposé et la structure documentaire
    - Document demandé par un client : *Politique de protection des données client*

Politiques de sécurité
Structure

Documents de gestion

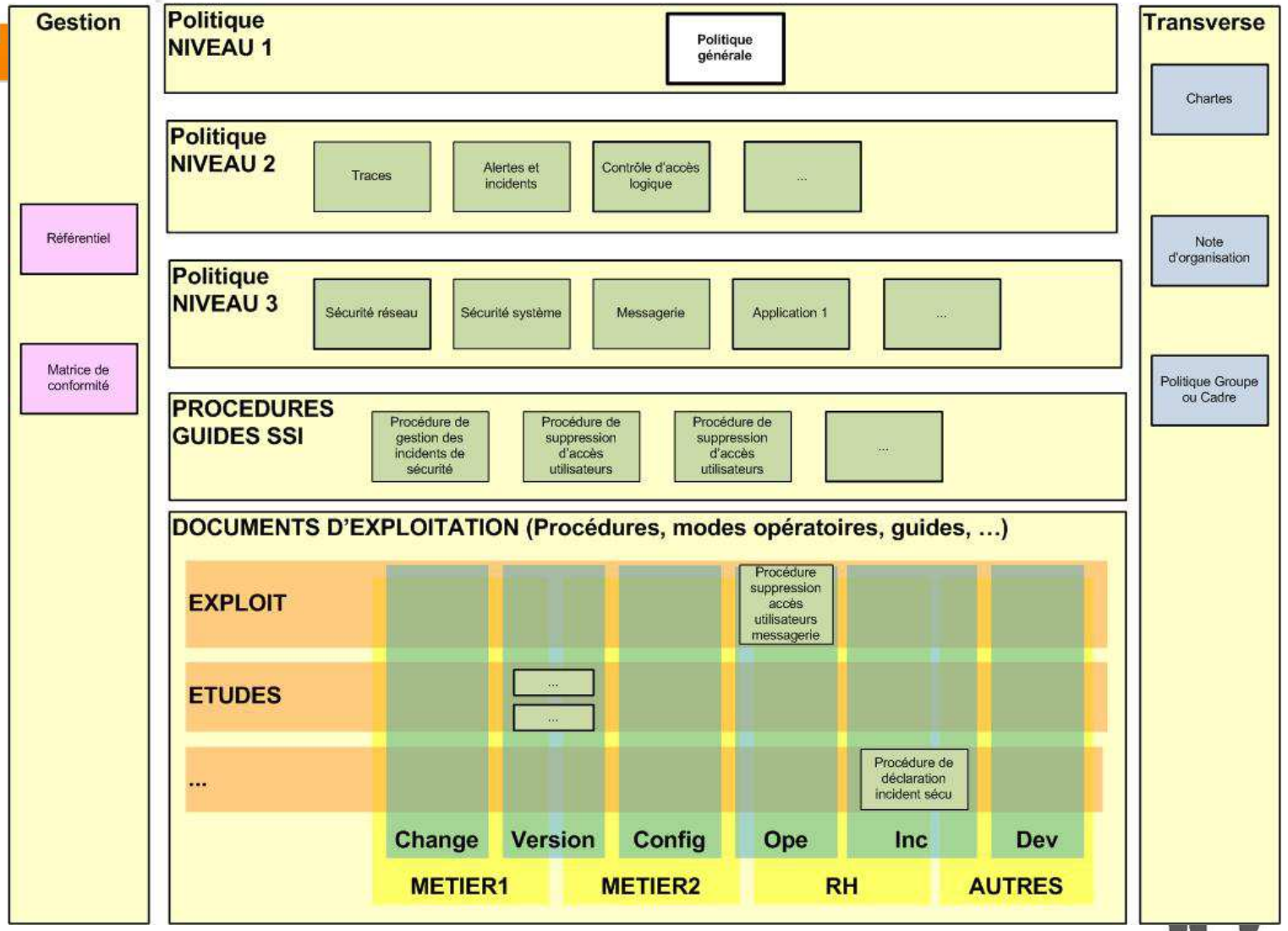
- Le référentiel documentaire
  - Contient notamment les « métadonnées » de la politique

Référence	Titre du document	Responsable du document		Publication - Diffusion				
		Fonction / Service	Nom - Prenom	Version	Statut	Date	Services / fonctions destinataires	Personnes destinataires
xxx	Politique de contrôle des accès logiques	RSSI		v2.0	Diffusé	12-mars	xxx	
xxx	Politique de gestion des traces, alertes et incidents	RSSI		v1.0	Non diffusé			
xxx	xxx			v1.0	Non diffusé			

Niveau 1 | Niveau 2 | Niveau 3 | Procédure | Transverse | Externe

- Le(s) documents de suivi de la « conformité »
  - Globale (Référentiel = N2)
  - Par « domaine » (Référentiel = N2) : Applications RH

Politiques de sécurité
Structure



Politiques de sécurité
Structure

Modèle documentaire

Table des matières

Politiques de sécurité
Rôles

- Rôles « génériques » relatifs à chaque document

		Exemples
Valider	Tout ou partie d'un document de politique (*ex : la stratégie de contrôle d'accès*)	Comité Sécurité, Directeur Général
Définir et mettre à jour		RSSI, Experts
Diffuser		RSSI
« Faire appliquer »		RSSI
Appliquer, Mettre en œuvre		Administrateurs, Chefs de projet,
Contrôler, vérifier		RSSI, Audit interne

Politiques de sécurité
Contenu

- Des règles ou exigences qui peuvent être en 2 parties :
  - Décrire ce qu'il faut faire
  - … et décrire ce qui a été fait !

2 Règles

2.1 Stratégie de contrôle d'accès

2.1.1 [redacted] et les différents types d'accès associés. [redacted]

[redacted]

Catégorie d'utilisateurs	Type d'accès autorisés	Type d'accès interdits
Personnels externes (visiteurs)	Accès wifi visiteurs	
Personnels externes sous contrats	Poste fixe ou nomade géré par l'organisme Accès communs (bureautique, messagerie, intranet, …) Accès aux applications métiers soumis à autorisation	Tout terminal non géré par la DSI Accès wifi visiteurs avec poste géré par l'organisme
Personnels sous responsabilité RH	…	…
…	…	…

2.3 Alertes et incidents de sécurité

2.3.1 Les critères d'identification des alertes et incidents de sécurité doivent être définis et maintenus [redacted]

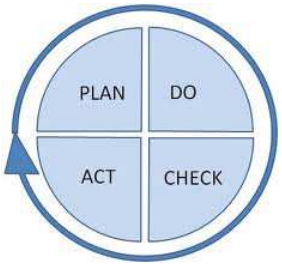
Alertes et incidents de sécurité – Critères [redacted] *(alerte ou incident de sécurité [redacted])*		
Critères	**Description**	**Exemple**
Type de ressource	*Toute alerte ou incident (arrêt, dysfonctionnement) lié à une fonction de sécurité ([redacted], antivirus, [redacted]…) ayant pour conséquence un [redacted]*	*Désactivation d'un antivirus*
Type de fonction	*Toute alerte ou incident relatif aux fonctions suivantes d'une ressource :* - [redacted] - [redacted]	*Tentative d'authentification infructueuse*
Origine	*Toute alerte ou incident [redacted] malveillante ou intentionnelle*	*Attaque SYN FLOOD*
Impact	*Toute alerte ou incident ayant un impact en termes de [redacted]*	*Fuite d'information*
Politique	*Toute alerte ou incident causé par ou ayant pour conséquence [redacted]*	*Attribution d'un accès sans autorisation*

Politiques de sécurité
Projet ou processus ?

- Un projet de définition de politique de sécurité, c'est bien …
  - « Une politique de sécurité sera définie à un instant t »

- … un projet de « définition et mise en œuvre d'un « *processus* » de gestion de politique de sécurité », c'est mieux !
  - Modalités de gestion de la politique : validation, mise à jour, diffusion, contrôle, …
  - De manière itérative et progressive

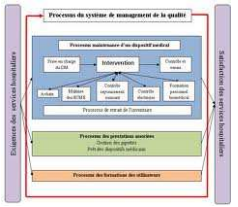
  « Ne pas tout faire d'un seul coup »



ISO/IEC 27001:2005

Politiques de sécurité
Mise en œuvre

- <u>Adaptation</u> à l'existant et aux besoins de l'organisme
  - Au niveau de la structure documentaire
    - Par rapport à la cartographie des processus
    - … en fonction du niveau de maturité
      - Processus RH ⇔ Politique RH ⇔ ~~Politique de sécurité RH~~ ?
      - Processus de gestion des tiers ⇔ ~~Politique de gestion des tiers~~ ⇔ Politique de sécurité des tiers ?
      - Continuité d'activité
      - Juridique / Réglementaire



  - Au niveau des activités de gestion
    - Validation : instances, comités
    - Diffusion : communication
    - Contrôle : audit interne

Politiques de sécurité
Mise en œuvre

- Impliquer les « acteurs » dans la définition / rédaction des politiques
  - « Valideur »
  - « Appliqueur »

- Sous forme de groupe de travail avec comme support une base « générique » de règles

- La « diffusion » des politiques doit être accompagnée d'actions de sensibilisation (« convaincre ») et de formations (« apprendre »)

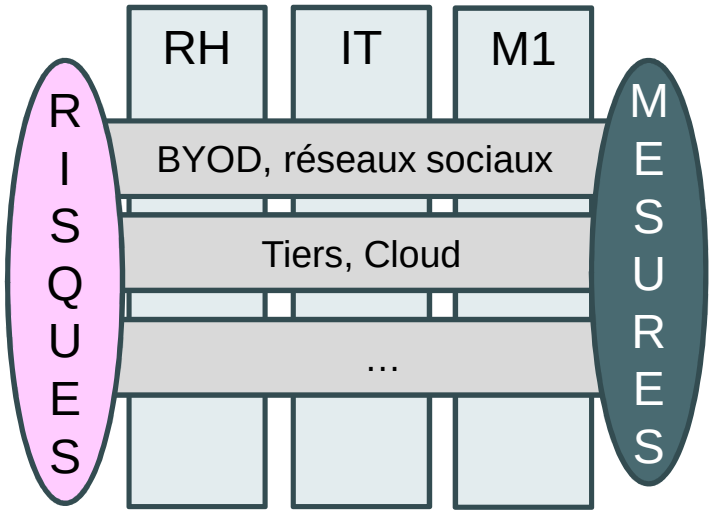
Politiques de sécurité et gestion des risques (1)

- « La politique de sécurité doit découler d'une analyse de risques »
  - La politique générale doit intégrer une description des enjeux principaux issues de l'analyse de risques globale à l'organisme
  - Les politiques de sécurité détaillées relatives aux domaines métiers / applicatifs doivent être élaborés en fonction des analyses de risques spécifiques. *Ex : nature ou durée de conservation de traces liées à des exigences métiers spécifiques, niveau de contrôle d'accès logique adaptée au niveau de sensibilité des données*

- L'évolution des politiques de sécurité dépends directement des évolutions du risque
  - Usages : *BYOD, réseaux sociaux, …*
  - Menaces : *DDOS, APT, …*

Politiques de sécurité et gestion des risques (2)

- Interfaces RISQUES ⇔ POLITIQUES



Politiques de sécurité
Conclusion

- « Plusieurs politiques de sécurité » …
  - La politique de sécurité interne qui décrit les règles et exigences s'appliquant à l'ensemble des activités de l'organisme

    Ex : Politique de sécurité relative à la gestion des tiers, Politique de protection des données, …

  - Des documents « périphériques » pouvant être intitulé « politiques de sécurité » destinés à répondre à des besoins spécifiques (souvent « externes »)

    Ex : Politique de sécurité applicable au tiers (à usage d'annexe contractuelle par exemple), Politique de protection des données clients

Politiques de sécurité
Conclusion

Point-clés	Et vous ?
Organisation, rôles, processus de gestion	?
Structure documentaire	?
Analyse de risques	?
Diffusion / Sensibilisation	?
Contrôle / Vérification / conformité	?
Complétude / profondeur	?

Merci de votre attention

?

http://www.scassi.com

Sébastien RABAUD – SCASSI Conseil
sebastien.rabaud@scassi.com