Sécurité des Systèmes d'Information
FSD & RSSI

Bertrand Wallrich, FSD & RSSI

INVENTEURS DU MONDE NUMÉRIQUE

AMUE – 28 Novembre 2012

SSI : un enjeu pour les FSD ?

- Conseil des ministres du 25 mai 2011 :

”Les attaques contre les systèmes d’information de l’État et des entreprises se multiplient partout dans le monde. Elles portent atteinte à la souveraineté des États, au patrimoine des entreprises et aux données personnelles des citoyens. De nouvelles menaces apparaissent qui visent les processus industriels. Elles pourraient mettre en danger les infrastructures vitales du pays et avoir des conséquences directes sur la vie quotidienne des Français et sur l’économie. »

http://www.elysee.fr/president/root/bank_objects/Compte-rendu_du_CDM_du_25_mai_2011.pdf

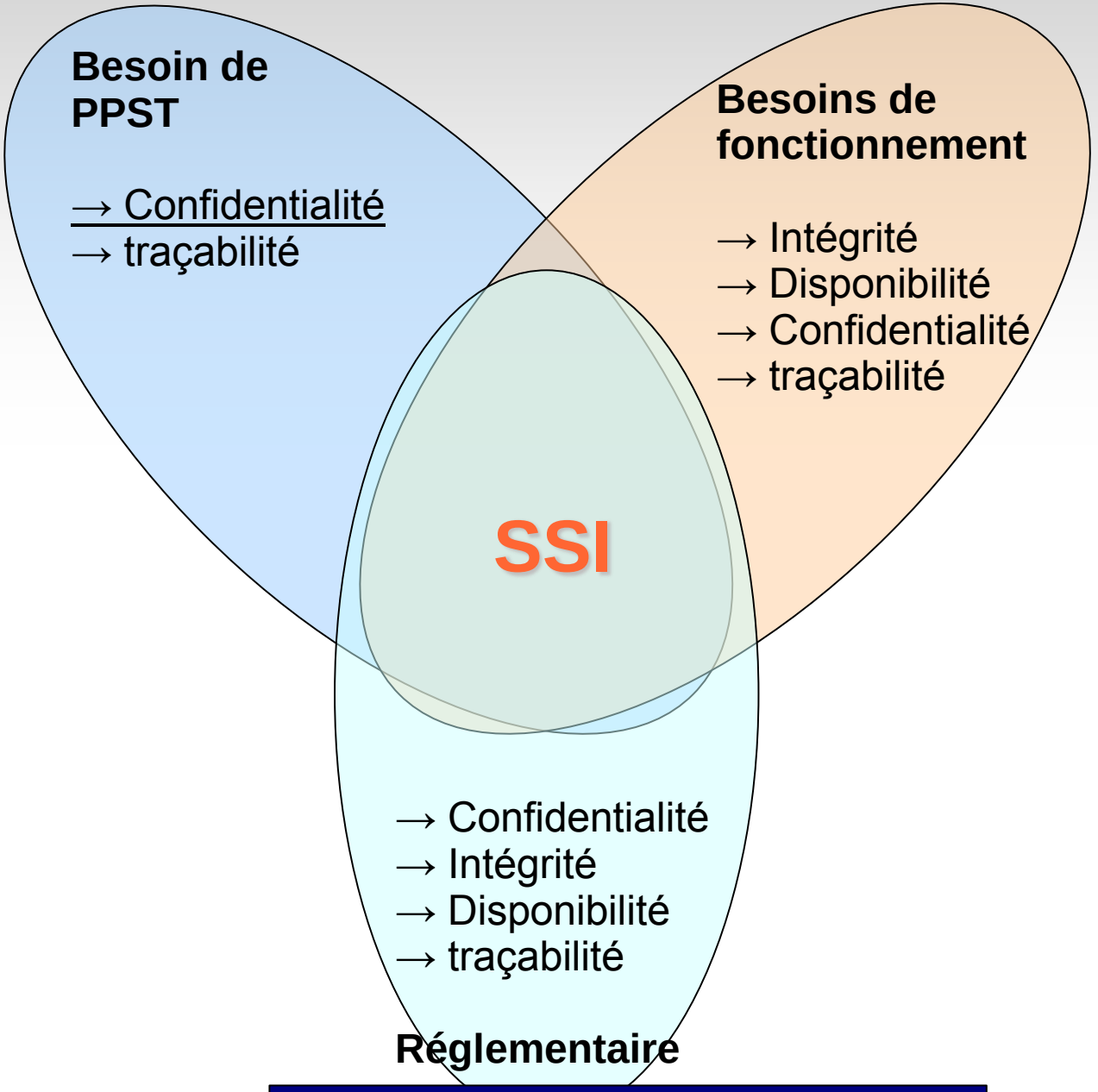
Le site de l'ANSSI

http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/defense-et-securite-des-systemes-d-information-le-gouvernement-annonce-un.html

⇒ Prise en compte de la SSI au plus haut sommet de l'état :

Le piratage informatique est un moyen d'accéder à des données sensibles, du savoir, des connaissances. Et son utilisation est une réalité.

Les enjeux sur la SSI



Protection du Potentiel Scientifique et Technologique

- Patrimoine de plus en plus sous forme électronique :
  - Thèses, brevets en cours, résultats d'expériences, données industrielles liées à des contrats, NDA, …
- Informations pour atteindre le patrimoine sur support électronique :
  - Gestion des accès physiques, rapports d'analyse, atteinte physique, …
- Un besoin de confidentialité :
  - ➔ Authentification (SSO, certificats, fédérations d'identités, …)
  - ➔ Gestion des droits d'accès (Droits fichiers, cloisonnements de zones, …)
  - ➔ Tracabilité (systèmes de gestion de trace, corrélation d'événements, …)

Protection du Potentiel Scientifique et Technologique

- Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation
- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation
- *"...l'accès à une zone à régime restrictif pour y effectuer un stage, y préparer un doctorat, y participer à une activité de recherche, y suivre une formation, y effectuer une prestation de service ou y exercer une activité professionnelle est soumis à l'autorisation du chef du service, d'établissement ou d'entreprise, après avis favorable du ministre chargé d'en exercer la tutelle... »*
  - Définir des zones en tenant compte des accès informatiques
  - Orthogonalité du physique et du logique :
    - Accès distants, VPN, Nomadisme, « Téléactivités »
    - Organisationnel :
      - Circuit validation compte et processus RH ?

Besoins de fonctionnement

- La DSI relaye des demandes des directions et des utilisateurs :
  - Un SI fiable (disponibilité) :
    - ➔ Antivirus, firewall, antispam …
  - Un SI fiable (intégrité) :
    Des données dont on est sûr de leur présence et de leur ”justesse”.
    - ➔ Sauvegardes, PCA, PRA
    - ➔ Signature numérique, ...
  - Un SI de confiance (confidentialité) :
    - ➔ AAA (*Authentication*, *Authorization*, *Accounting/Auditing*)

Règlementation (1/2)

- Arrêté du 23 juillet 2010 portant approbation de l'IGI sur la protection du secret de défense national (*http://www.ssi.gouv.fr/IMG/pdf/iqi1300.pdf*) :

Etendu à la notion de « Diffusion Restreinte » et ses implications en terme de SSI

"les informations doivent être chiffrées à l'aide d'un dispositif ayant fait l'objet d'une qualification au niveau standard, d'une caution de l'ANSSI ou d'une évaluation par le centre d'expertise technique SSI du ministère. »

- CNIL (Loi Loi 78-17 du 6 janvier 1978 modifiée)

"Article 34

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

Règlementation (2/2)

Référentiel général de sécurité (version 1.0 du 6 mai 2010) (*http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/*):

Notion de « qualification » des produits et prestataires

Extrait du [DécretRGS] : Chapitre II : Fonctions de sécurité des systèmes d'information :

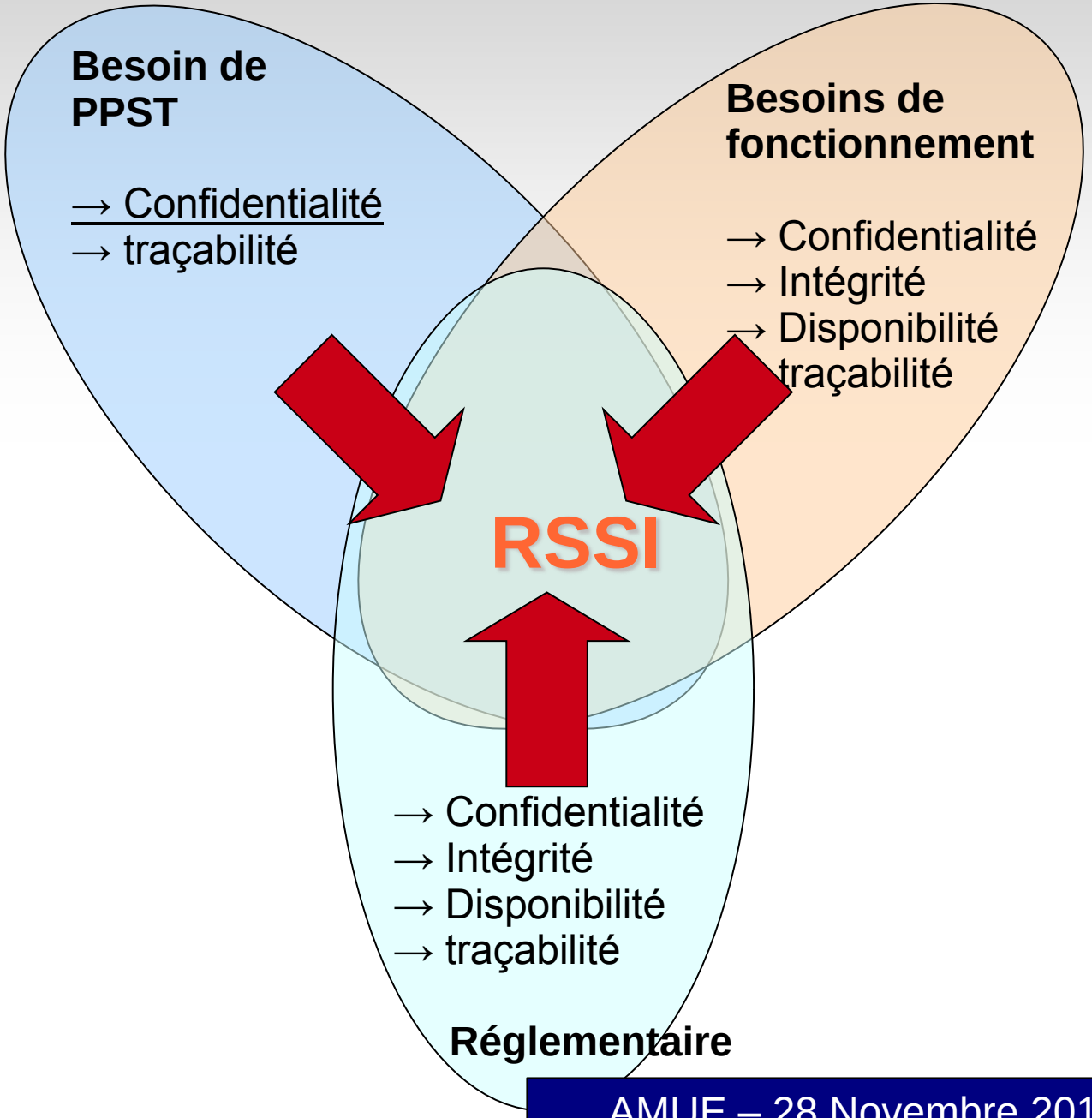
« Article 4 :

Pour mettre en oeuvre dans un système d'information les fonctions de sécurité ainsi déterminées, l'autorité administrative recourt à des produits de sécurité et à des prestataires de services de confiance ayant fait l'objet d'une qualification dans les conditions prévues au présent décret ou à tout autre produit ou prestataire pour lesquels elle s'est assurée de la conformité de leurs fonctions de sécurité au référentiel général de sécurité. »

- Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

"Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article. »

Les enjeux sur la SSI



Tout ne peut pas être pris en compte :

→ Politique de sécurité.

Définir les organisations,
les rôles, les enjeux principaux,
Identifier et évaluer les risques ;
définir des règles ;
élaborer un plan d'actions

→ Une sécurité gérée.

Management de la SSI,
indicateurs, évolutivité de la PSSI.

FSD et SSI ?

Questions réccurentes :

- Quel doit-être le rôle du FSD dans la sécurité des systèmes d'information ?
  - En maîtrise d'ouvrage ?
  - En maîtrise d'oeuvre ?
  - Indépendance ?
- Le FSD et le RSSI doivent-il être :
  - En lien hiérarchique ?
  - Au même niveau dans l'organigramme ?
- Le ministère (HFDS) impose-t-il une organisation ?
- Les textes, lois et normes, permettent-elle de se positionner ?
- ...

Guides :

- Textes de loi
- Instruction interministérielles
- RGS
- Normes : ISO 2700X
- Guides, recommandations

Positionnement FSD

Les différents rôles au sein d'un établissement, en lien avec la SSI :

- AQSSI (Autorité qualifiée)
- AA (Autorité administrative)
- FSD
- AH (Autorité d'homologation)
- RSSI / ASSI / OSSI (*Officier de SSI*)
- CSSI (Correspondant SSI)
- RMSI (Responsable Management de Sécurité)
- CIL (Correspondant informatique et liberté)
- ...

- CPS (Comité de pilotage stratégique de la SSI)
- CSO (Comité de sécurité opérationnel)
- CL (Comité de liaison)
- DSI
- ...

Positionnement FSD

Les différents rôles au sein d'un établissement, en lien avec la SSI :

- AQSSI (Autorité qualifiée)
- AA (Autorité administrative)

} Directeur de l'établissement

- FSD
- AH (Autorité d'homologation)
- RSSI / ASSI / OSSI (*Officier de SSI*)
- CSSI (Correspondant SSI)
- RMSI (Responsable Management de Sécurit
- CIL (Correspondant informatique et liberté)
- ...

Pilote au niveau stratégique la SSI.

Valide la PSSI,
Fait les choix concernant les risques majeurs.
Réunion 1 fois par an.

- CPS (Comité de pilotage stratégique de la SSI)
- CSO (Comité de sécurité opérationnel)
- CL (Comité de liaison)
- DSI
- ...

Positionnement FSD

Les différents rôles au sein d'un établissement, en lien avec la SSI :

- AQSSI (Autorité qualifiée)
- AA (Autorité administrative
- FSD
- AH (Autorité d'homologati
- RSSI / ASSI / OSSI (*Officier de SSI*)
- CSSI (Correspondant SSI)
- RMSI (Responsable Management de Sécurité)
- CIL (Correspondant informatique et liberté)
- ...

Manage la SSI.

Position de MOA. Effectue le lien avec le CPS.
Gère au quotidien la PSSI, son évolution (roue de Deming)

- CPS (Comité de pilotage stratégique de la SSI
- CSO (Comité de sécurité opérationnel)
- CL (Comité de liaison)
- DSI
- ...

Pilote de manière opérationnelle la SSI.

coordonner les activités quotidiennes liées à la sécurité

Réunion min 3 fois par an.

Positionnement FSD

Les différents rôles au sein d'un établissement, en lien avec la SSI :

- AQSSI (Autorité qualifi
- AA (Autorité administr
- FSD
- AH (Autorité d'homologation)
- RSSI
- CSSI (Correspondant SSI)
- RMSI (Responsable M
- CIL (Correspondant
- ...
- CPS (Comité de pil
- CSO (Comité de séc
- CL (Comité de liaison)
- DSI
- ...

Mise en œuvre

Position de MOE.
Mise en œuvre de la PSSI et en assure le suivi et la gestion.

Pilote avec les correspondants des composantes (CSSI)

relais des décisions de sécurité au niveau d'une composante
Pilote les projets de sécurité, recueillent les problématiques d'implémentation de la sécurité, des incidents.

Réunion une fois par mois.

Positionnement FSD

Les différents rôles au sein d'un établissement, en lien avec la SSI :

- AQSSI (Autorité qualifiée)
- AA (Autorité administrative)
- FSD
- AH (Autorité d'homologation)
- RSSI
- CSSI (Correspondant SSI)
- MSI (Responsable Management de Sécurité)
- Correspondant informatique et liberté)
- ...

Homologue des solutions de sécurité.

Valide la sécurité d'un système, d'une plateforme...

Garant de la conformité à la CNIL.

Mise en œuvre au sein d'une composante.

Position de MOE.
Mise en œuvre de la PSSI et en assure le suivi
et la gestion localement.

Positionnement FSD/RSSI

	AQSSI	AA	FSD	CIL	AH	RMSI	DSI	RSSI	CSSI
Comité									
Comité de pilotage stratégique (CPS)	V	V	C	C	C	P			
Comité de sécurité opérationnelle (CSO)			C	C	C	V	C	P	
Comité(s) de liaison (CL)								P	C
Documents									
politique de sécurité	V (dans CPS)	V (dans CPS)	C (dans CPS)	C (dans CPS)	C (dans CPS)	P (dans CPS)	C	C	C
Shéma directeur de la SSI	V (dans CPS)	V (dans CPS)	C (dans CPS)	C (dans CPS)	C (dans CPS)	P (dans CPS)	C	C	C
Guides et documents d'application de la SSI					V (dans CSO)	V (dans CSO)	C	P (dans CSO)	C
Actions									
Définir et mettre en oeuvre les plans d'action, les mesures de sécurité					V (dans CSO)	V (dans CSO)	C	P (dans CSO)	C
Maintenir l'établissement en conformité aux référentiels			V (dans CSO)	V (dans CSO)	C	V (dans CSO)	C	P (dans CSO)	C
Suivi des plan d'actions (tableaux de bord), coordination					C	V (dans CSO)	C	P (dans CSO)	C
Organisation d'audits					V (dans CSO)	P (dans CSO)	C	C	C
Lien avec les tutelles (bilan annuel, incidents)			V ou P (dans CSO)	V ou P (dans CSO)	C	V ou P (dans CSO)	C	C	C
Formation et sensibilisation			C		C	V (dans CL)	C	P (dans CL)	C
Gérer les incidents de sécurité			C			V (dans CL)	C	P (dans CL)	C
veille technique et juridique			C	C	C	C	C	P (dans CL)	C

Légende

V: Valide, décide.
C: Contribue.
P: Pilote.

- Risque lié au pilotage et validation par la même personne
- Niveau stratégique
- Niveau décisions opérationnelles
- Niveau terrain

Cas détaillé des rôles

Positionnement FSD/RSSI

	AQSSI	AA	FSD	CIL	AH	RMSI = RSSI	DSI	RSSI = RMSI	CSSI
Comité									
Comité de pilotage stratégique (CPS)	V	V	C	C		P		P	
Comité de sécurité opérationnelle (CSO)			C	C	C	PV	C	PV	
Comité(s) de liaison (CL)						P		P	C
Documents									
politique de sécurité	V (dans CPS)	V (dans CPS)	C (dans CPS)	C (dans CPS)		PC (dans CPS)	C	C	C
Shéma directeur de la SSI	V (dans CPS)	V (dans CPS)	C (dans CPS)	C (dans CPS)		PC (dans CPS)	C	C	C
Guides et documents d'application de la SSI						PV	C	PV	C
Actions									
Définir et mettre en oeuvre les plans d'action, les mesures de sécurité						PV	C	PV	C
Maintenir l'établissement en conformité aux référentiels			V (dans CSO)	V (dans CSO)	C	PV (dans CSO)	C	PV (dans CSO)	C
Suivi des plan d'actions (tableaux de bord), coordination						PV (dans CSO)	C	PV (dans CSO)	C
Organisation d'audits					V (dans CSO)	P (dans CSO)	C	C	C
Lien avec les tutelles (bilan annuel, incidents)			V ou P (dans CSO)	V ou P (dans CSO)	C	V ou P (dans CSO)	C	C	C
Formation et sensibilisation					C	PV (dans CL)	C	PV (dans CL)	C
Gérer les incidents de sécurité						PV (dans CL)	C	PV (dans CL)	C
veille technique et juridique			C	C	C	P (dans CL)	C	P (dans CL)	C

Légende

V: Valide, décide.
C: Contribue.
P: Pilote.

Risque lié au pilotage et validation par la même personne
Niveau stratégique
Niveau décisions opérationnelles
Niveau terrain

Le RMSI et le RSSI sont mutualisé

Positionnement FSD/RSSI

	AQSSI	AA	FSD	CIL	AH	RMSI	DSI	RSSI	CSSI
Comité									
Comité de pilotage stratégique (CPS)	V	V	PC	C		PC			
Comité de sécurité opérationnelle (CSO)			V	C	C	V	C	P	
Comité(s) de liaison (CL)								P	C
Documents									
politique de sécurité	V (dans CPS)	V (dans CPS)	PC (dans CPS)	C (dans CPS)		PC (dans CPS)	C	C	C
Shéma directeur de la SSI	V (dans CPS)	V (dans CPS)	PC (dans CPS)	C (dans CPS)		PC (dans CPS)	C	C	C
Guides et documents d'application de la SSI			V (dans CSO)			V (dans CSO)	C	P (dans CSO)	C
Actions									
Définir et mettre en oeuvre les plans d'action, les mesures de sécurité			V (dans CSO)			V (dans CSO)	C	P (dans CSO)	C
Maintenir l'établissement en conformité aux référentiels			V (dans CSO)	V (dans CSO)	C	V (dans CSO)	C	P (dans CSO)	C
Suivi des plan d'actions (tableaux de bord), coordination			V (dans CSO)			V (dans CSO)	C	P (dans CSO)	C
Organisation d'audits			P (dans CSO)		V (dans CSO)	P (dans CSO)	C	C	C
Lien avec les tutelles (bilan annuel, incidents)			V ou P (dans CSO)	V ou P (dans CSO)	C	V ou P (dans CSO)	C	C	C
Formation et sensibilisation			V (dans CL)		C	V (dans CL)	C	P (dans CL)	C
Gérer les incidents de sécurité			V (dans CL)			V (dans CL)	C	P (dans CL)	C
veille technique et juridique			C	C	C	C	C	P (dans CL)	C

Légende

V: Valide, décide.
C: Contribue.
P: Pilote.

Risque lié au pilotage et validation par la même personne
Niveau stratégique
Niveau décisions opérationnelles
Niveau terrain

Le FSD et le RMSI sont mutualisé

Positionnement FSD/RSSI

	AQSSI	AA	FSD	CIL	AH	RMSI	DSI	RSSI	CSSI
Comité									
Comité de pilotage stratégique (CPS)	V	V	C	C		P			
Comité de sécurité opérationnelle (CSO)			C	C	C	V	P	P	
Comité(s) de liaison (CL)							P	P	C
Documents									
politique de sécurité	V (dans CPS)	V (dans CPS)	C (dans CPS)	C (dans CPS)		P (dans CPS)	C	C	C
Shéma directeur de la SSI	V (dans CPS)	V (dans CPS)	C (dans CPS)	C (dans CPS)		P (dans CPS)	C	C	C
Guides et documents d'application de la SSI						V (dans CSO)	P (dans CSO)	P (dans CSO)	C
Actions									
Définir et mettre en oeuvre les plans d'action, les mesures de sécurité						V (dans CSO)	P (dans CSO)	P (dans CSO)	C
Maintenir l'établissement en conformité aux référentiels			V (dans CSO)	V (dans CSO)	C	V (dans CSO)	P (dans CSO)	P (dans CSO)	C
Suivi des plan d'actions (tableaux de bord), coordination						V (dans CSO)	P (dans CSO)	P (dans CSO)	C
Organisation d'audits					V (dans CSO)	P (dans CSO)	C	C	C
Lien avec les tutelles (bilan annuel, incidents)			V ou P (dans CSO)	V ou P (dans CSO)	C	V ou P (dans CSO)	C	C	C
Formation et sensibilisation					C	V (dans CL)	P (dans CL)	P (dans CL)	C
Gérer les incidents de sécurité						V (dans CL)	P (dans CL)	P (dans CL)	C
veille technique et juridique			C	C	C	C	P (dans CL)	P (dans CL)	C

Légende

V: Valide, décide.
C: Contribue.
P: Pilote.

	Risque lié au pilotage et validation par la même personne
	Niveau stratégique
	Niveau décisions opérationnelles
	Niveau terrain

Le RSSI est rattaché à la DSI

Positionnement FSD/RSSI

	AQSSI	AA	FSD	CIL	AH	RMSI	DSI	RSSI	CSSI
Comité									
Comité de pilotage stratégique (CPS)	V	V	C	C		P			
Comité de sécurité opérationnelle (CSO)			C	C	C	PV	PV	PV	
Comité(s) de liaison (CL)							PV	PV	C
Documents									
politique de sécurité	V (dans CPS)	V (dans CPS)	C (dans CPS)	C (dans CPS)		P (dans CPS)	C	C	C
Shéma directeur de la SSI	V (dans CPS)	V (dans CPS)	C (dans CPS)	C (dans CPS)		P (dans CPS)	C	C	C
Guides et documents d'application de la SSI						PV	PV	PV	C
Actions									
Définir et mettre en oeuvre les plans d'action, les mesures de sécurité						PV	PV	PV	C
Maintenir l'établissement en conformité aux référentiels			V (dans CSO)	V (dans CSO)	C	PV (dans CSO)	PV (dans CSO)	PV (dans CSO)	C
Suivi des plan d'actions (tableaux de bord), coordination						PV (dans CSO)	PV (dans CSO)	PV (dans CSO)	C
Organisation d'audits					V (dans CSO)	P (dans CSO)	P (dans CSO)	P (dans CSO)	C
Lien avec les tutelles (bilan annuel, incidents)			V ou P (dans CSO)	V ou P (dans CSO)	C	V ou P (dans CSO)	C	C	C
Formation et sensibilisation					C	PV (dans CL)	PV (dans CL)	PV (dans CL)	C
Gérer les incidents de sécurité						PV (dans CL)	PV (dans CL)	PV (dans CL)	C
veille technique et juridique			C	C	C	P (dans CL)	P (dans CL)	P (dans CL)	C

Légende

V: Valide, décide.
C: Contribue.
P: Pilote.

Risque lié au pilotage et validation par la même personne

Niveau stratégique

Niveau décisions opérationnelles

Niveau terrain

le RMSI = RSSI est dans la DSI

Conclusion : FSD / RSSI

D'autres considérations sont à prendre en compte :

- Une organisation avec les personnes existantes, leurs compétences ?
- Importance de la SSI dans la PPST ?
- Des affichages simples, une communication claire : un interlocuteur unique ?
- De l'ampleur de la PSSI et des chantiers à mener ?

FSD / RMSI / RSSI - Un travail d'équipe :

- Pour des objectifs atteignables (ex : se méfier des interdictions trop fortes et contournées),
- Pour une cohérence de l'ensemble (ex : accès physiques vs accès logiques, partage de l'importance des enjeux),
- Pour choisir le niveau le plus adéquat (ex : confluence d'intérets),
- Pour gérer les cas transverses (ex : piratage informatique et PPST)

- En évitant ou tenant en compte les risques ”juge et partie”

ANNEXES

- Définition AQSSI (Arreté du 23 juillet 2010)

Les autorités qualifiées sont responsables de la sécurité des systèmes d'information au niveau d'un service, d'une direction d'un ministère, au niveau d'un organisme ou d'un établissement relevant d'un ministère. Les autorités qualifiées sont désignées par le ministre pour le département et les organismes dont il a la charge. Leur responsabilité ne peut être déléguée. En liaison avec le HFDS et le FSSI du département ministériel dont elle relève, l'autorité qualifiée est notamment chargée :

de définir, à partir des objectifs de sécurité qu'elle fixe, ou, pour les systèmes traitant d'informations classifiées, des objectifs de sécurité fixés par la présente instruction, une politique de sécurité des systèmes d'information adaptée à son service, sa direction, son établissement ou son organisme ;

de s'assurer que les dispositions réglementaires et, le cas échéant, contractuelles sur la sécurité des systèmes d'information sont appliquées, notamment celles relatives à la sécurité des systèmes traitant d'informations classifiées ;

de faire appliquer les consignes et les directives internes ;

de s'assurer que des contrôles internes de sécurité sont régulièrement effectués ;

d'organiser la sensibilisation et la formation du personnel aux questions de sécurité, en particulier en matière de systèmes d'information ;

de s'assurer de la mise en œuvre des procédures réglementaires prescrites pour l'homologation des systèmes, pour l'agrément des dispositifs de sécurité et pour la gestion des articles contrôlés de la sécurité des systèmes d'information (ACSSI) (147) ;

de désigner les autorités d'homologation des systèmes relevant de sa responsabilité.

Dans le cas d'un organisme qui ne relève pas d'un ministre, notamment un organisme privé, il appartient au responsable de cet organisme de désigner, en son sein, une personne ayant la fonction d'autorité qualifiée au sens du présent article.

ANNEXES

Définition RSSI (Arreté du 23 juillet 2010)

- Les autorités qualifiées peuvent se faire assister par un ou plusieurs agents, responsables ou officiers de sécurité des systèmes d'information (ASSI, RSSI, OSSI) (148). Elles précisent, lors de leur désignation, le périmètre de leurs attributions et leur dépendance hiérarchique. Ce périmètre peut être un service, une direction ou un organisme, dans sa totalité, ou un ou plusieurs systèmes d'information, ou un établissement.
- Ces agents assurent principalement les fonctions opérationnelles de la sécurité des systèmes d'information. Ils peuvent être notamment chargés :
  - d'être les contacts privilégiés des utilisateurs du système pour les questions de sécurité ;
  - d'assurer la formation et la sensibilisation des responsables, des informaticiens et des usagers en matière de sécurité des systèmes d'information ;
  - de tenir à jour la liste des personnels ayant accès aux systèmes d'information ;
  - de faire surveiller en permanence les activités des personnes extérieures appelées à effectuer des interventions sur les systèmes d'information ;
  - de s'assurer de l'application, par les personnels d'exploitation et les utilisateurs, des règles de sécurité prescrites ;
  - d'assurer leur sensibilisation aux mesures de sécurité et de les informer de toute modification des conditions d'emploi du système ;
  - de veiller à la mise en œuvre des mesures de protection prescrites, d'établir des consignes particulières et de contrôler leur application ;

ANNEXES

- Définition de la mission de RSSI suivant le CIGREF (nomenclature 2002)
  - Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il peut intervenir directement sur tout ou partie des systèmes informatiques et télécoms de son entité. Il effectue un travail de veille technologique et réglementaire sur son domaine et propose des évolutions qu'il juge nécessaires pour garantir la sécurité logique et physique du système d'information dans son ensemble. Il est l'interface reconnu des exploitants et des chefs de projets mais aussi des experts et des intervenants extérieurs pour les problématiques de sécurité de tout ou partie du SI. Le RSSI est généralement rattaché à la direction informatique.

- RGS : Responsable de la sécurité des systèmes d'information (RSSI)
  - En fonction des organismes, le RSSI, ou la personne faisant office de RSSI, peut avoir différents rattachements. Rattaché à la direction générale, il est chargé de proposer la politique de sécurité du système d'information (PSSI) qui sera fixée par l'AA, et de veiller à son application. Dans le cadre d'un projet, il conseille l'autorité d'homologation. Rattaché à la direction informatique, il intervient en tant qu'expert auprès de la direction de projet et valide les livrables SSI au regard de la PSSI. Dans le cadre du processus d'homologation de sécurité d'un système d'information, il a la charge de présenter l'analyse de risques.

ANNEXES

- Évolution des missions du RSSI lié à la maturité de l'entreprise à la sécurité de l'information

  – Dans certaines grandes entreprises, on voit apparaître deux missions correspondant au partage des responsabilités du RSSI entre deux interlocuteurs : l'un pour la maîtrise d'œuvre, et l'autre pour la maîtrise d'ouvrage :

    - Le CISO (Chief Information Security Officer), a une mission centrée sur la gestion des risques (Risk Manager) et l'organisation de la sécurité. Il participera aux réunions du Comité de Direction.
    - Le RSSI (Responsable Sécurité des Systèmes d'Information) a la responsabilité opérationnelle d'appliquer les règles à l'ensemble du domaine informatique. Il disposera d'un savoir-faire d'architecte technique de la sécurité et d'une parfaite connaissance des processus et des systèmes d'information.

  – A chief security officer (CSO) is a corporation's top executive who is responsible for security.

The CSO generally serves as the business leader responsible for the development, implementation and management of the organization's corporate security vision, strategy and programs. They direct staff in identifying, developing, implementing and maintaining security processes across the organization to reduce risks, respond to incidents, and limit exposure to liability in all areas of financial, physical, and personal risk; establish appropriate standards and risk controls associated with intellectual property; and direct the establishment and implementation of policies and procedures related to data security.

Digital security is involved in physical security. At many companies a CSO is the person responsible for IT security, the term CSO was first used principally to designate responsibility of IT security and is still used in this way.