THALES

THALES SERVICES S.A.S.

SECURITE DES SYSTEMES D'INFORMATION

MISSION ET ORGANISATION

TABLE DES MATIERES

1. PRESENTATION DU DOCUMENT

1.1 OBJET

Le présent document décrit l'organisation ainsi que les missions et responsabilités de la fonction Sécurité des Systèmes d'Information (SSI) de Thales Services (TS) sur les périmètres d'entreprises et étatique, c'est-à-dire relatifs aux classifications de Thales et de l'état (NP, DR, CD, SD et leurs équivalents.

Il détaille notamment les activités de l'équipe SSI de Thales Services, l'organigramme de la fonction SSI, et les rôles et responsabilités de la chaine SSI.

1.2 DOCUMENTS APPLICABLES

Les documents applicables sont :

- [1] : Note Organisation - Thales Services (83320005-GOV-CIS)
- [2] : Note d'organisation de la Direction des Systèmes d'Information (DSI) de TS (83320100-GOV-CIS)
- [3] : Mission et Organisation de la Direction de l'Ingénierie IT Outsourcing (83320030-GOV-CIS)
- [4] : Mission et Organisation de la Direction de l'Ingénierie Logiciel (83320113-GOV-CIS)
- [5] : Mission et Organisation de la Direction Sites, Sécurité et Etablissement (83320072-GOV-CIS)
- [6] : Politique Générale de la Sécurité des Systèmes d'Information (PGSSI) de Thales Services (83320093-GOV-CIS)

1.3 ACRONYMES

- AQSSI : Autorité Qualifiée SSI
- CODIR : Comité de Direction
- COPIL : Comité de Pilotage
- CS : Centre de Services
- CSSI : Correspondant SSI
- CVSSI : Comité de Validation SSI et de suivi des exceptions de Sécurité
- DEV : Développement
- DIL : Direction Ingénierie Logiciel
- DIO : Direction Ingénierie IT Outsourcing
- DPO : Data Protection Officer
- DSI : Direction des Systèmes d'Information
- GRC : Gouvernance Risques et Contrôles de la SSI

- OCS : Officier Central de sécurité (physique)
- OCSSI : Officier Central Sécurité Systèmes d'Information
- OS : Officier de sécurité (physique)
- OSSI : Officier Sécurité Systèmes d'Information
- PAS : Plan d'assurance sécurité
- PGSSI : Politique Générale de Sécurité des Systèmes d'Information
- PSSI : Politique de Sécurité des Systèmes d'Information
- RIE : Réseau Informatique d'Entreprise
- RSSI : Responsable Sécurité Système Information
- SSI : Sécurité des Systèmes d'Information
- SMSI : Système de Management de la Sécurité des Systèmes d'Information (cf. ISO 27001)
- TS : Thales Services SAS

2. ORGANISATION DE LA FONCTION SSI

2.1 LA FONCTION SECURITE DES SI

Le périmètre d'activité de la fonction SSI de TS porte sur tous les aspects Sécurité des Systèmes d'Information (SSI) portés au sein des activités de Thales Services pour ses clients ou pour lui-même, que ce soit dans un cadre public (étatique) ou privé.

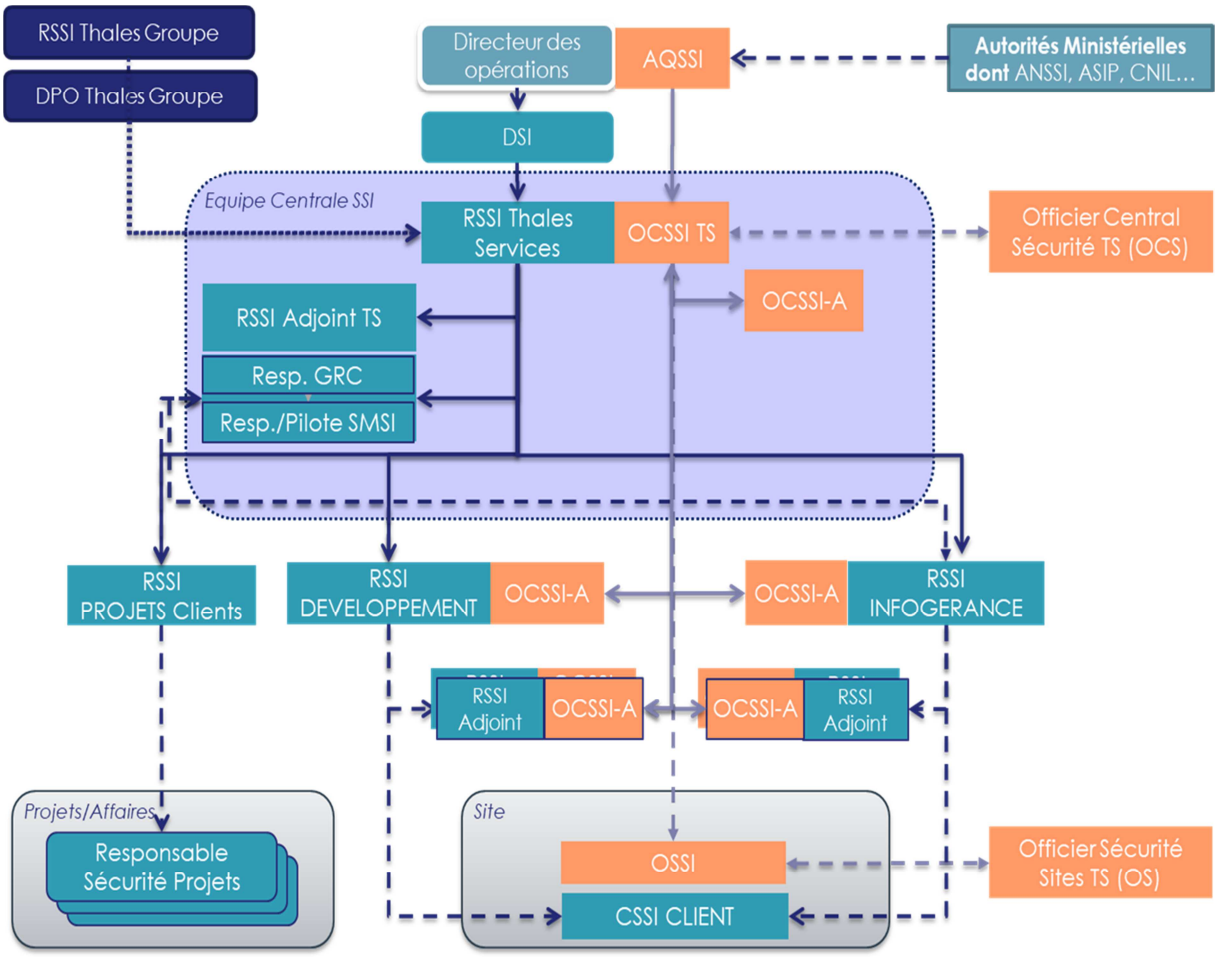
C'est pourquoi le RSSI de TS est également l'OCSSI de Thales Services.

Conformément aux termes de la Politique Générale SSI (PGSSI) de TS [DA6], la fonction SSI de TS est responsable de la définition de la stratégie de la sécurité des systèmes d'information, et de sa déclinaison opérationnelle.

Cette fonction est notamment chargée de piloter, de décliner de manière opérationnelle, et de contrôler la mise en œuvre des différentes Politiques de Sécurité des SI (PSSI) de TS.

Thales Services est engagée depuis 2016 dans une démarche ISO 27001. A cet effet TS dispose d'un SMSI qui couvre l'ensemble des différents périmètres certifiés ISO 27001 de TS sous la responsabilité du RSSI de TS.

2.2 SCHEMA D'ORGANISATION DE LA SSI TS



3. LA CHAINE SSI DE THALES SERVICES

3.1 L'EQUIPE SSI CENTRALE

L'équipe centrale est en charge des activités de GRC et de pilotage du SMSI. Elle est rattachée au RSSI de Thales Services.

3.1.1 LE RESPONSABLE SECURITE DES SYSTEMES D'INFORMATION

Le Responsable Sécurité des systèmes d'information (RSSI) de Thales Services est chargé :

- de définir la stratégie de sécurité des systèmes d'information à déployer sur les dispositifs organisationnels et techniques portant les activités d'infogérance et de développement de Thales Services,
- d'analyser périodiquement le différentiel entre le niveau d'exigence formulé par Thales Services et la situation réelle, et d'en déduire des plans d'action sécurité pluriannuels, ainsi que les moyens (budgétaires et organisationnels) associés,
- de s'assurer au travers de la fonction de contrôle permanent dont il valide la stratégie, de la bonne application des PSSIs et de leurs déclinaisons opérationnelles, et de gérer toutes les exceptions de sécurité,
- d'assurer le reporting auprès de la direction de Thales Services,
- de mettre en place une organisation SSI efficiente et permettant en particulier de réduire les risques au strict minimum,
- d'exprimer auprès du responsable sécurité physique de Thales Services les exigences (règles des PSSIs) pour protéger les actifs informationnels de Thales Services et de ses clients, en cohérence avec les prescriptions de sécurité physique du Groupe Thales.

Il porte :

1. La responsabilité de faire appliquer les prescriptions SSI du Groupe Thales,
2. Au titre de sa fonction de Responsable SMSI, il assure les missions déclinées au § 3.1.4,
3. Au titre de sa fonction d'OCSSI, il assure les missions déclinées au § 4.2**Erreur ! Source du renvoi introuvable.**.

Le RSSI de Thales Services est rattaché hiérarchiquement au Directeur des Systèmes d'Information (DSI), qui porte les risques SSI de l'entreprise, et fonctionnellement au RSSI du Groupe.

3.1.2 LE RSSI TS ADJOINT

Le RSSI TS Adjoint seconde le RSSI de Thales Services pour toutes les missions qu'il lui confie, il assure la suppléance de cette fonction, et il veille au bon fonctionnement de la GRC (Gouvernance Risques Contrôles).

Ses principales missions sont de :

- Contribuer à l'élaboration de la politique SSI de l'entreprise,
- Assister le RSSI TS dans le pilotage de la SSI du quotidien de son périmètre en :
  - Remontant les nouvelles menaces et en collectant les besoins Sécurité,
  - S'assurant de la mise à jour de l'analyse des risques TS (AdR) et de la DDA,
  - Contribuant à la gouvernance et à l'animation de la communauté SSI métier,
  - Contribuant ou traitant des incidents de sécurité des SI.

Il rapporte au RSSI de Thales Services.

Au sein de Thales Services, les RSSIs Adjoints ont également la fonction d'Officier Central de Sécurité des Systèmes d'Informations Adjoint (OCSSI-A) sur leur périmètre.

A ce titre, le RSSI Adjoint TS assiste le RSSI TS et les RSSI métiers à maintenir la conformité SSI des SI et réseaux sensibles de Défense de leur périmètre au regard de la réglementation de Défense. Il rapporte hiérarchiquement à l'OCSSI de TS.

3.1.3 LE RESPONSABLE DE LA GRC

Le responsable de la GRC est en charge des activités SSI se rapportant à la Gouvernance (G), au traitement des Risques (R) et aux Contrôles (C) (de niveau 2).

3.1.3.1 La Gouvernance SSI

Les activités de Gouvernance (G) SSI portent sur les domaines suivants :

- L'élaboration de la PGSSI, sa déclinaison en politiques (PSSI), en notes d'organisation, en instructions et documentations associées,
- La mise en place des différents processus de sécurité, leur accompagnement et leur revue,
- La contribution à l'acquisition et au maintien des agréments et certifications,
- La réalisation, la tenue et la revue du socle documentaire SSI,
- La veille de conformité SSI légale et réglementaire,
- La consolidation des indicateurs et tableaux de bord SSI,
- L'organisation et l'animation des comités de direction SSI (CODIR SSI-TS),
- La participation aux actions de sensibilisations.

3.1.3.2 Le Risque SSI

Les activités sur le Risque (R) portent sur les domaines suivants les domaines suivants :

- Garantir la bonne exécution, le suivi et la mise à jour des analyses de risques SSI de Thales Services,
- Définir et maintenir la méthodologie d'analyse et de traitement de risques,
- Apporter un support à l'utilisation de la méthodologie d'analyse de risques,
- Consolider le TOP 10 des risques.

3.1.3.3 Le Contrôle SSI

Le Contrôle (C) permanent SSI s'assure que l'on couvre bien les risques SSI identifiés par l'analyse de risque de l'année en cours.

C'est une étape essentielle du Système de Management de la Sécurité des Systèmes d'Information, permettant d'avoir une assurance raisonnable de la bonne maitrise des risques SSI et de vérifier concrètement la bonne application :

- des politiques de sécurité des SI (PSSI) de Thales Services et de leurs directives associées,
- des mesures de sécurité contribuant au maintien de nos certifications (ISO 27001; HDS),
- des processus de sécurité internes de Thales Services.

Dans ce cadre, le responsable de la GRC propose chaque année une stratégie de contrôles efficiente.

Il s'assure également de :

- la bonne définition du plan de contrôles,
- la bonne exécution du plan de contrôles,

- de la cohérence et de la qualité du résultat des contrôles.

Le responsable de la GRC est rattaché au RSSI de Thales Services.

3.1.4 LE RESPONSABLE DU SMSI

La responsabilité du SMSI est placée sous l'autorité du Responsable Sécurité des Systèmes d'Information de Thales Service (RSSI TS), chargé de :

- Définir et proposer des orientations stratégiques et des objectifs d'amélioration pour le SMSI,
- Assurer un reporting auprès de la Direction, et animer la Revue de Direction du SMSI,
- Maintenir et entretenir les activités et la cohérence du SMSI sur les périmètres certifiés,
- Veiller à l'atteinte des objectifs de sécurité fixés,
- De gérer les processus liés à la certification ISO 27001 (AdR, PTR, DdA, support à audit, suivi des plans d'actions et de remédiation),
- Proposer, avec le pilote du SMSI, son plan annuel de contrôle SSI,
- Gérer avec le pilote SMSI / Contrôler l'exécution du plan de contrôle, et du reporting des contrôles de niveau 2,
- Exercer un devoir d'alerte en cas de dérive / dysfonctionnements majeurs du SMSI,
- Gérer les relations avec les parties prenantes du SMSI.

D'un point de vue opérationnel, il fait valider les risques résiduels et le plan de traitement des risques par le Directeur des Systèmes d'Information (DSI).

Pour exercer sa mission, le Responsable SMSI peut déléguer certaines de ces activités à un Pilote SMSI.

3.1.4 LE PILOTE DU SMSI

Les activités du pilote SMSI sont les suivantes :

- Garantir l'application, le respect et le déploiement en interne du SMSI (communication et sensibilisation internes et gestion des ressources),
- Définir et maintenir les documents du SMSI (gestion des évolutions, modifications et traçabilité),
- Contribuer avec le responsable du SMSI et le responsable GRC à la réactualisation des risques,
- Suivre le plan de traitement des risques, les non-conformités afférentes au SMSI, et les plans d'action SSI,
- Définir et faire évoluer les indicateurs de pilotage et le reporting associé,
- Gérer les interfaces du SMSI et les conventions de services associées,
- Préparer et animer les Comités du SMSI et Revue de Direction du SMSI.

Au titre de la fonction de contrôle permanent :

- Contribuer à la définition du Plan de Contrôle annuel,
- Collecter les résultats des contrôles de niveau 1 et les preuves associées,
- Assurer le support du niveau 1 vis-à-vis des équipes opérationnelles pour un bon déploiement des contrôles en liaison avec les CSSI locaux,
- Consolider les résultats des contrôles, analyser et produire les synthèses à destination du management permettant d'estimer la couverture des risques sur leur périmètre.

Il est sous la responsabilité fonctionnelle du Responsable SMSI.

3.2 LA SECURITE SUR LES PRESTATIONS CLIENTES

La sécurité sur les Prestations Clientes est transverse, elle s'assure au sein des affaires et projets que l'assurance sécurité est bien délivrée. Pour cela, en étroite collaboration avec les RSSI Métiers, la sécurité clients suit les indicateurs et plans d'actions des COSECs et s'assure de la bonne résolution des incidents et/ou investigations de sécurité.

3.2.1 LE RSSI PROJETS CLIENTS

Le RSSI PROJETS Clients est chargé :

- d'animer la chaine des Responsables Sécurité Projets (RSP) sur tous les périmètres d'activité de Thales Services,
- de participer au recrutement et à la qualification des RSP,
- de l'affectation des ressources en RSP en fonction d'une part des exigences des clients, et d'autre part des offres retenues pour ces affaires,
- d'assurer le support et l'escalade managériale pour les RSP sur des affaires ou des problématiques clients plus complexes, et nécessitant une expertise plus avancée,
- de valider les livrables des RSP (RAO, BUILD et RUN),
- de proposer aux Programs Managers l'évolution des offres retenues en fonction des retours des clients,
- de proposer au RSSI de Thales Services les éventuelles évolutions du contenu des offres SSI proposées aux clients,
- de déployer les outils de suivi de l'assurance sécurité (COSECs) sur les affaires et d'assurer un reporting sécurité des affaires / clients,
- de fournir au RSSI TS des indicateurs et rapports lui permettant d'évaluer le niveau de risque résiduel lié à la Cyber-menace sur nos prestations clientes (Niveau d'Assurance Sécurité).

Il rapporte au RSSI de Thales Services.

3.2.2 LES RESPONSABLES SECURITE PROJETS (RSP)

Le **RSP assure un rôle d'analyse et d'évaluation du respect des exigences sécurité** lors de toute évolution d'un périmètre de service. À cette fin il joue un rôle primordial dans plusieurs phases d'activité.

Il est l'interface SSI des BID Manager (RAO), PDA (RAO, BUILD, RUN), Project Manager (BUILD), PM et SDM (RUN).

En phase de RAO : Le RSP apporte son soutien aux équipes de BID à l'évaluation des exigences de sécurité, et, via la rédaction du PAS, à la réponse technique et organisationnelle à y apporter. Il est l'interlocuteur privilégié du BID Management et du PDA. Il valide le niveau de risque SSI du projet.

Pour les RAO où il n'y a pas de RSP nommé, c'est le BID Manager qui est garant du niveau de risque SSI de la réponse et de la formalisation l'assurance sécurité, matérialisée par un PAS.

En phase BUILD : le RSP :

- est l'interface du RSSI du client. Il s'appuie, pour ce faire, sur un Responsable Opérationnel Sécurité, ou à défaut sur le Project Manager Build pour établir le reporting du chantier sécurité qu'il communique.

- participe à la réunion de Build to Run (mise en production, livraison au client) et effectue la recette de sécurité. Il émet un avis SSI pour le passage en Run des projets (via le modèle du CVSSI). En cas de non-conformité, il évalue le risque et alerte le management du programme et le RSSI TS.
- rédige les documents liés à la gouvernance sécurité du projet (Plan d'Assurance Sécurité (PAS)). Il conseille le Project Manager sur les points en lien avec la sécurité du projet. Il accompagne le projet dans sa préparation aux différents comités de validation de sécurité (CVSSI, CFSSI).
- assiste le Project Manager en pilotant l'assurance sécurité du projet, notamment en :
  - s'assurant de la sécurité des environnements de BUILD et du bon niveau de MCS,
  - collectant les besoins Sécurité de la solution et veillant à ce que les mesures sécurité couvrent les nouvelles menaces et vulnérabilités,
  - s'assurant de l'effectivité des mesures de sécurité et de leur mise en œuvre,
  - contribuant à la gouvernance et à l'animation SSI du projet (sensibilisation, information, validation des créations et clôtures de comptes à privilèges sur le projet, collecte et formalisation des alertes et incidents SSI, production d'un tableau de bord)
  - contribuant ou traitant des incidents de sécurité ou alertes SSI.

Pour les offres où il n'y a pas de RSP nommé, c'est le Project Manager qui est garant au titre du contrat de l'assurance sécurité, matérialisée par une synthèse de type COSEC.

Les RSP sont rattachés fonctionnellement au RSSI PROJETS Clients et au Project Manager dans le cadre de leurs activités dans un contrat.

En phase RUN : le RSP assure le rôle de RSA, décrit dans le Groupe Thales, et il :

- est l'interface du RSSI du client,
- A partir des éléments fournis par la chaîne opérationnelle (SDM et ses équipes, le responsable de la MCS ou le responsable sécurité opérationnel s'ils sont nommés sur le projet), le RSP analyse, puis communique le rapport sécurité de l'activité de Run via les planches COSEC.
- assiste le Program Manager en pilotant l'assurance sécurité de la prestation délivrée au titre du contrat, en :
  - s'assurant de la sécurité des environnements de RUN et du bon niveau de MCS,
  - collectant les besoins Sécurité du Client et veillant à ce que les mesures sécurité couvrent les menaces et vulnérabilités,
  - s'assurant de l'effectivité des mesures de sécurité et de leur mise en œuvre,
  - contribuant ou traitant des incidents de sécurité ou alertes SSI,
  - contribuant à la gouvernance et à l'animation SSI du contrat (sensibilisation, information, validation des créations et clôtures de comptes à privilèges sur le projet, production d'un tableau de bord),
  - mettant à jour le plan d'assurance sécurité.

Pour les offres où il n'y a pas de RSP nommé, c'est le Program Manager qui est garant au titre du contrat de l'assurance sécurité, matérialisée par une synthèse de type COSEC.

Les RSP sont rattachés fonctionnellement au RSSI PROJETS Clients et au Program Manager dans le cadre de leurs activités dans un contrat.

3.3 LA SECURITE METIERS

En plus de la sécurité transverse « Clients » décrite au §3.2, l'organisation SSI de Thales Services s'appuie sur deux domaines métiers principaux, l'infogérance (DIO) et le développement (DIL).

L'infogérance est principalement orientée sur la sécurisation des infrastructures réseaux et systèmes et du MCO/MCS associés ; le Développement s'attache à sécuriser ses solutions (secure by design), ses méthodes de développements et de maintenance ; la sécurité des environnements de développement repose sur des prestations infogérées.

La SSI métiers est pilotée par un RSSI assisté de RSSI adjoints. Ils sont chargés de mettre en place une chaîne SSI dans leur métier, composée d'un réseau de CSSIs locaux.

3.3.1 LE RSSI METIER

Le RSSI Métier est chargé de :

- Contribuer à l'élaboration de la politique SSI de l'entreprise, et au maintien des politiques et directives de son périmètre,
- s'assurer de la déclinaison opérationnelle de la PSSI de Thales Service et de la PSSI sectorielle[1] afférente à son activité (Infogérance ou Développement), et de leur bonne application en exécutant des contrôles de niveau 2 sur son périmètre,
- Gérer les demandes des validations SSI des solutions et architectures de son périmètre, ainsi que les exceptions temporaires et le suivi de leurs mesures compensatoires,
- Tenir à jour un tableau de bord SSI et le communiquer régulièrement au RSSI de Thales Services,
- Assister le RSSI de Thales Services dans le pilotage de la SSI du quotidien de son périmètre en :
  - Remontant les nouvelles menaces et collectant les besoins Sécurité,
  - S'assurant de la mise à jour l'analyse des risques TS (AdR) et la DDA,
  - Contribuant à la gouvernance et à l'animation de la communauté SSI métier,
  - Contribuant ou Traitant des incidents de sécurité des SI.

Ils sont assistés dans leurs tâches par des RSSI Adjoints.

Les RSSI Métier (Infogérance et Développement) sont rattachés hiérarchiquement au RSSI de TS.

3.3.2 LE RSSI METIER ADJOINT

La mission principale d'un responsable sécurité des systèmes d'information métier adjoint est d'assister le RSSI Métier dans la mise en œuvre de l'ensemble des processus nécessaires à la protection des données et des systèmes d'information de son périmètre d'activité.

Dans le cadre de ses fonctions il 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 périmètre.

Agissant en coordination étroite avec un RSSI Métier (Infogérance / Développement), sur plusieurs sites, son rôle et ses missions sont de :

- Assister le RSSI Métier et les OSSI de sites pour assurer la conformité des SI de son périmètre au regard des lois et des réglementations de défense,
- Contribuer à l'élaboration des documents liés aux « Accréditations de Site » et à la rédaction des divers dossiers SSI,
- Contribuer à l'élaboration de la politique SSI de l'entreprise et à sa déclinaison en directives de sécurité,

[1] Les PSSI sectorielles sont des PSSI complémentaires à la PSSI / TS permettant d'adresser les sujets spécifiques au métier.

- Assister le RSSI Métier dans le pilotage de la SSI du quotidien de son périmètre,
- Vérifier la bonne application sur son périmètre de la PSSI Thales Services (TS) et des directives de sécurité en collaboration avec les CSSI locaux et conformément aux objectifs SSI,
- Proposer en collaboration avec les équipes expertes SI des actions correctives le cas échéant, voire suivre leur mise en œuvre.

Le RSSI adjoint Métier a un lien hiérarchique avec le RSSI de Thales Services et est fonctionnellement rattaché au RSSI métier (Infogérance, Développement).

Le RSSI adjoint Métier a la fonction d'Officier Central de Sécurité des Systèmes d'Informations adjoint (OCSSI-A) de son métier de rattachement.

A ce titre, il est garant de l'application de la réglementation de Défense en matière de SSI sur son domaine pour les réseaux sensibles et classifiés de Défense.

Au titre de sa fonction d'OCSSI-A, il rapporte fonctionnellement à l'OCSSI de Thales Services.

3.3.3 LES CORRESPONDANTS SSI LOCAUX

Pour l'essentiel, le Correspondant Sécurité des Systèmes d'Information (CSSI) est le référent de sécurité de son centre de services et/ou de son site, il facilite et contrôle la bonne application de la PSSI, et il participe si nécessaire à sa déclinaison opérationnelle en lien avec le RSSI de son domaine d'activité.

Le CSSI s'appuie sur le socle documentaire SSI mis à disposition par l'équipe centrale. Il suit également les exceptions de sécurité de niveau local, et il valide les droits d'accès des comptes à hauts privilèges des personnels rattachés à son centre de services. Il assure par ailleurs les sensibilisations SSI, et il suit les incidents de sécurité de son domaine d'activité.

Le CSSI est supporté dans ses activités par la chaîne SSI et rattaché fonctionnellement à un RSSI Métier (Infogérance / Développement).

4. MISSION ET ORGANISATION SSI SUR LE PERIMETRE ETATIQUE

4.1 L'AUTORITE QUALIFIEE SSI (AQSSI)

Le RSSI adjoint Métier a la fonction d'Officier Central de Sécurité des Systèmes d'Informations adjoint (OCSSI-A) de son métier de rattachement.

Pour les systèmes d'information sensibles[2] ou classifiés de l'état, les attributions de l'AQSSI de Thales Services sont les suivantes :

- définir, en cohérence avec la politique SSI ministérielle, des objectifs et une politique de sécurité de sécurité des systèmes d'information pour les systèmes traitant d'informations sensibles ou classifiées, adaptée à TS,
- s'assurer pour ces systèmes d'information que les dispositions réglementaires et le cas échéant contractuelles sur la sécurité des systèmes d'information sont appliquées,
- faire appliquer les consignes et les directives internes,
- s'assurer que des contrôles internes de sécurité sont régulièrement effectués,
- organiser la sensibilisation et la formation du personnel aux questions de sécurité, en particulier en matière de sécurité de systèmes d'information,
- 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),
- prononcer les homologations sur les SI sensibles ou classifiés de l'état.

4.2 L'OFFICIER CENTRAL DE SECURITE DES SYSTEMES D'INFORMATION

Placé sous l'autorité de l'AQSSI, l'Officier Central Sécurité des systèmes d'information (OCSSI) exerce une autorité fonctionnelle sur l'ensemble des Officiers Sécurité des Systèmes d'Information (OSSI) de sites dépendant de l'AQSSI, et il veille au travers de contrôles SSI réguliers au respect de la bonne réalisation des missions des OSSI placés sous sa responsabilité.

Il est également le conseiller de l'AQSSI pour tout ce qui se rapporte aux homologations de sécurité des clients étatiques pour les SI sensibles ou classifiés et aux obligations légales et réglementaires afférentes. Il peut réaliser des contrôles portant sur la bonne application des règles / exigences de sécurité formulées.

En étroite coordination avec l'Officier Central (OCS) de Thales Services, l'OCSSI s'assure de la bonne application de la réglementation étatique concernant la protection des informations sensibles et classifiées sur les systèmes d'information hébergés et/ou infogérés par Thales Services pour le compte de ses clients étatiques.

L'OCSSI s'adresse à l'OCS pour l'obtention de toute annexe de sécurité utile au Maintien en Condition de Sécurité (MCS) du système d'information d'un client étatique ayant décliné sous cette forme ses exigences de sécurité, pour compléter ou préciser les règles à respecter.

Il est aidé dans sa tâche par des adjoints fonctionnels (OCSSI-A) par région et par métier.

[2] SI sensibles = Il s'agit généralement d'environnement DR (Diffusion Restreinte) étatiques mais la notion de sensible désigne également le DRSF (DR Spécial France) et PSTN (Potentiel scientifique et Technique de la Nation).

4.3 LES OFFICIERS CENTRAUX DE SECURITE DES SYSTEMES D'INFORMATION ADJOINT (OCSSI-A)

Les Officiers Centraux de Sécurité des Systèmes d'Information Adjoints (OCSSI-A) assistent l'OCSSI de Thales Services pour les missions qu'il leur confie, et supportent les OSSIs locaux dans leurs tâches (et faisant donc fonction d'OSSI-A sur les dossiers traités).

4.4 L'OFFICIER DE SECURITE DES SYSTEMES D'INFORMATION

Les Officiers Sécurité des Systèmes d'Information (OSSI) sont les contacts privilégiés des utilisateurs du système d'information sensible ou classifié pour les questions de sécurité.

Il est chargé :

- 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 sensibles ou classifiés,
- de faire surveiller en permanence les activités des personnes extérieures appelées à effectuer des interventions sur les systèmes d'information,
- de veiller au respect des procédures opérationnelles de sécurité, à la mise en œuvre des mesures de protection prescrites, et d'établir des consignes particulières et de contrôler leur application,
- d'assurer la gestion, la comptabilité et le suivi des ACSSI dans leur périmètre de responsabilité, et d'en assurer périodiquement l'inventaire,
- d'établir les consignes de sécurité relatives à la conservation, au stockage et à la destruction des ACSSI,
- de rendre compte de toute anomalie constatée ou de tout incident de sécurité.

En particulier, l'OSSI exprime auprès des Officiers de Sécurité (OS) de site les besoins suivants :

- Fourniture de locaux aptes à opérer des systèmes d'information classifiés,
- Fourniture des habilitations des personnes,
- Fourniture et gestion des droits d'accès physiques aux locaux classifiés et sensibles.

Les OSSI rapportent fonctionnellement à l'OCSSI.

5. INTERACTION SSI AVEC LES PHASES BID, BUILD ET RUN

La SSI est une activité transverse, tout Thales Services est acteur de sa sécurité.

Les RACI ci-dessous permettent d'illustrer les points clés de la SSI qui doivent être adressés par les équipes et managers opérationnels de TS. La SSI de TS s'appuie ainsi sur des tiers pour les réaliser ses missions lors des phases de BID, BUILD, RUN et contrôle.

Réalisateur (R) : Celui (personne ou équipe) qui réalise l'activité.
Approbateur (A) : Celui qui arbitre toutes les décisions sur l'activité. C'est aussi celui qui conçoit l'activité, définit les modalités de déroulement, peut décider d'arrêter, reprendre ou d'annuler l'activité.
Consulté (C) : Celui qui est consulté pendant l'activité par le réalisateur. Il peut aussi apporter un support en transverse de l'activité dans le cadre de sa mission de conseil.
Informé (I) : Celui qui est informé du déroulement et du résultat de l'activité par le réalisateur.

Plusieurs profils Clés contribuent à la sécurité des systèmes d'information durant ces phases :

- La Direction
- Les intervenants du BID
  - Capture Leader,
  - BID Manager.
- Les intervenants BUILD et RUN
  - Projet : Programme Manager (PM), Service Delivery Manager (SDM), ou Project Manager ;
  - Design Authority (et Project Design Authority).
- Les intervenants Opérationnels
  - Operational Manager : Responsable Application /Manager d'équipes Infogérance, de développement et de ressources, et responsable MCS.
  - Administrateurs et Experts Technique.
- La SSI
  - RSSI et CSSI,
  - RSSI PROJETS Clients et RSP.
- Les départements Supports et fonctions transverses
  - Achats,
  - Juridique,

BID	Direction	Capture Leader	BID Mgr	DA /PDA	RSSI	RSP	Achats	Juridique
Qualifier les besoins de sécurité de l'offre y compris celui des ressources habilités (questionnaire / RFP)	A	R	C	C	C			
Evaluer le risque SSI pour TS et définir les objectifs et offres de sécurité de l'affaire/projet (questionnaire / Offre)	A	I	R	C	I	C		
Fournir le plan d'assurance sécurité (PAS)		I	R	I	A	C		I
Sélections d'un fournisseur		I	A	C	I	C	R	I
Intégrer les exigences de sécurité de l'offre au contrat		I	R		A	C		C

BUILD	Direction	PROJET	DA / PDA	Manager	Expert	RSSI	RSP	Achats
Définition et suivi du plan projet (organisation projet, E/S, nom du RSP) (Prévention)	A	R	C	C		I	C	
Sélections de sous-traitants		A		C		I	C	R
Sensibilisation et Habilitation des collaborateurs (Prévention)		A		C		I	R	
Gestion des exigences de sécurité et des contrôles associés (Prévention)		A	C	C	C	I	R	
Inclusion des exigences de sécurité IS dans les procédures opérationnelles et identification des preuves associées (N1)		A	C	R	C	I	C	
Suivi MCS (Détection)		A		C	C	I	R	
Gestion des investigations et incidents de sécurité SI du projet (Réaction)		A			C	I	R	
Production des indicateurs SSI (Tableaux de bord COSEC et reporting)	I	A	I	I	R	I	C	
Validation des fonctions de sécurités de la solution et de la couverture des besoins CIDT (i.e Hardening, AV, Pentest, Codes Review…)		A	C		C	I	R	
Mise en production et VSR		A		I	R	I	C	

RUN	Direction	PROJET	Manager	Infogerance	RSSI	RSP
Fournir le MCO/MCS		A	C	R	I	I
Analyse et Reporting SSI		I	I	C	A	R
Gestion des droits d'accès en veillant à la séparation des rôles		A	C	R	I	I
Respect de la couverture du besoin sécurité (y compris lors de changement - CAB)	I	A		C	I	C
Gestion des vulnérabilités SSI techniques (A12.6.1)		A	I	R	I	C
Gestion des incidents de sécurité	I	A	I	R	I	C

6. INSTANCES DE GOUVERNANCE SSI

La comitologie de la chaîne SSI est déclinée sur 3 niveaux :

- **Direction :** un Comité de Direction pour l'ensemble de la gouvernance SSI TS, définition des objectifs de sécurité, assurance sécurité, préparation de la revue de direction et des interventions en CODIR TS. Une revue de direction avec l'ensemble des parties prenantes est également réalisée une fois par an.
- **RSSI :** avec des Comités de Pilotage par métier (infogérance, développement, Clients) et préparation des interventions en CODIR Métier.
- **LOCAL :** avec la tenue de Comités Sécurité (COSEC) pour la gestion opérationnelle SSI (partage d'indicateurs, suivi du MCS et des plans d'actions SSI) dans les entités et BUs ;

En marge de ces comités, une gouvernance (CVSSI), pilotée par un RSSI de TS, est mise en place pour s'assurer de la bonne prise ne compte des besoins sécurité dans la définition des solutions mise en production sur le périmètre SIP de TS. Cette gouvernance se traduit par la tenue mensuelle d'un comité de validation SSI qui vérifie la conformité du traitement des risques SSI de ces solutions et suit le cas échéant les dérogations induites par un non-respect temporaire d'exigences de sécurité.

Comité	objectifs	Frequence
CODIR SSI	Piloté par la SSI TS ▸ Suivi des revues des risques SSI et maintien en condition des politiques ▸ Suivi des déploiements politiques de sécurité ▸ Revue des indicateurs et tableau de bord (Maturité, Risques, alertes et incidents) ▸ Validation des Plans d'actions SSI	▸ Trimestriel
COPIL SSI	Piloté par le RSSI ▸ Consolidation et suivi des alertes et incidents ▸ Mise en œuvre des Objectifs SSI sur le périmètre ▸ Suivi du Plan de traitement des risques ▸ Suivi Entrées/Sorties -accès –sensibilisation-circuits arrivée-départ	▸ Mensuel
COSEC (par Client, CS, Région DEV)	Piloté par un CSSI ▸ Déploiement des politique ▸ Suivi des Indicateurs sécurité (PAS) ▸ Suivi des Alertes/Incidents ▸ Suivi des non conformités et plans d'action ▸ Suivi des actions de communication	▸ Mensuel

6.1 REVUE DE DIRECTION

La Revue de Direction (RDD[3]) du SMSI a pour objectif d'**examiner le Système de Gestion de la Sécurité de l'Information de Thales Services** afin de s'assurer que celui-ci soit **pertinent, adéquat et efficace** à l'égard des exigences de la norme ISO 27 001 puis du référentiel HDS et qu'il constitue un levier d'**amélioration continue au profit de la satisfaction des clients et de la performance.**

[3] RDD = Revue de direction, aussi appelée Management Review.

6.2 COMITE DE DIRECTION – CODIR SSI-TS

Le **CODIR SSI-TS** assure la gouvernance de la fonction SSI de Thales Services, en validant les analyse de risques, définissant les objectifs de Sécurité, en suivant et arbitrant les plans d'actions SSI et en veillant à l'atteinte des objectifs de sécurité de SI.

Le mode de fonctionnement du CODIR-SSI est fondé sur un travail collaboratif assurant un déploiement cohérent de la PGSSI et des PSSIs au sein de Thales Services, à les enrichir, à coordonner les actions transverses, à analyser les dysfonctionnements majeurs (incidents de sécurité, déviations de sécurité, anomalies de fonctionnement des dispositifs, etc.), à capitaliser sur les solutions et à maintenir en condition de sécurité (MCS) les dispositifs de sécurité en place.

Le CODIR-SSI-TS est présidé par le RSSI de Thales Services, et il se réunit au moins une fois par trimestre et, selon les événements, sur décision du RSSI de Thales Services.

Il est composé de membres permanents :

- Le responsable de la GRC.
- Les RSSIs de TS (INFOGERANCE, DEV, PROJETS Clients),
- Le Responsable du SMSI,

Et en fonction des sujets :

- Le Pilote SMSI,
- Les RSP,
- Les Correspondants SSI (CSSI),
- Des invités.

6.3 COMITE DE PILOTAGE (COPIL)

Le Comité de Pilotage a en charge le suivi, la coordination et assure l'amélioration continue du système de management du SI. Le Comité assure le suivi opérationnel des incidents / mesures de sécurité (implémentées ou à mettre en place).

Fréquence : Le COPIL est de fréquence à minima bimensuelle.

Participants : Il est organisé et présidé par un RSSI.

6.4 COMITE DE SECURITE COSEC

Le **COSEC** assure la gestion de la sécurité au sein de chaque périmètre, et il permet de traiter spécifiquement les sujets SSI en cours intéressant l'activité concernée. Parmi les sujets qui doivent être traités au sein de ce COSEC, figurent obligatoirement, le suivi des divers plans d'action portant sur la SSI, ainsi que le suivi des incidents de sécurité avec les éventuelles améliorations à proposer pour éviter qu'ils ne se reproduisent, ainsi que la remontée des indicateurs.

Fréquence : Les COSEC se réunissent à minima bimestriellement en cohérence avec la planification des COPILs afférents.

Participants : Le COSEC est organisé et animé par un CSSI.

6.5 COMITE DE VALIDATION SSI - CVSSI

Le **CVSSI** est une instance de décision du niveau central de Thales Services, qui permet de valider des choix techniques de sécurité, des modifications d'architectures impactant la sécurité, ou pour formuler des exigences de sécurité avant l'acquisition de produits de sécurité.

Il permet aussi de suivre toutes les non-conformités afin de valider les éventuelles exceptions de sécurité avec une échéance de mise en conformité afférente. La validation SSI peut aussi être réalisée dans le cadre d'une revue d'architecture.

Fréquence : Le CVSSI se réunit mensuellement ou sur demande du RSSI de Thales Services.

Participants : Il est composé à minima d'un RSSI (Thales Services ou métier), ainsi que des éventuels chefs de projets, architectes et responsables de production concernés par la demande de validation.

THALES

CONTROLE DE REVISION

Version	Date	Auteur	Modification
001	17/10/17	Pascal PERRET	Création
002	03/10/18	Pascal PERRET	Revue annuelle
003	07/02/20	Philippe COULON	Evolution de l'organisation
004	01/09/20	Philippe COULON	Mise à jour suite à nouvelle organisation Thales Services

APPROBATION

	Nom	Titre	Date	Signature
Responsable	**Philippe COULON**	**RSSI de Thales Services**	– –	Signature numérique de COULON Philippe Date : 2020.09.16 11:29:13 +02'00'
Validation	**Eric OLLIVIER** **Elodie SEGUIN**	**Directeur des Systèmes d'Information** **Directeur Qualité et Satisfaction Client**	– – – –	OLLIVIER Eric Signature numérique de OLLIVIER Eric Date : 2020.09.29 15:34:39 +02'00' Signature numérique de SEGUIN Elodie Date : 2020.09.21 10:21:21 +02'00'
Approbation	**Anne FIGUEREO**	**Directrice des opérations de Thales Services**	– –	Signature numérique de FIGUEREO Anne Date : 2020.09.29 16:43:13 +02'00'

ATTENTION : Si ce document a été imprimé, contrôlez sa validité en consultant la dernière version en vigueur sur l'Intranet.

Toutes remarques et propositions d'évolution du contenu de ce document doivent être adressées à :

Thales Services S.A.S
Direction Qualité et Relation Client