POLITIQUE GENERALE DE SECURITE DU SYSTEME D'INFORMATION DU TRESOR PUBLIC

Version : 1.00

Date : 7 avril 2005

SOMMAIRE

Préambule

Le Trésor Public s'est engagé dans un contrat pluriannuel de performance qui marque sa volonté de devenir l'opérateur comptable et financier de référence en :

- renforçant la qualité des procédures comptables ;
- améliorant et développant les prestations vis-à-vis des usagers et des partenaires ;
- favorisant un pilotage actif du réseau du Trésor Public de nature à encourager une plus grande efficacité interne.

Face à de tels enjeux, le système d'information (SI) du Trésor Public joue un rôle de tout premier plan :

- il contribue à la traçabilité des opérations et augmente la transparence de la gestion publique ;
- il est au centre de programmes stratégiques visant à développer l'administration fiscale électronique et à moderniser les moyens de paiement ;
- il fournit aux agents les informations nécessaires au pilotage des activités et à la maîtrise de la qualité de service.

À ce titre, le SI, qui contient et traite de multiples données sensibles (financières, contractuelles, relatives aux usagers, aux partenaires et aux agents), doit être préservé de toute menace (panne, accident, erreur, malveillance) au même titre que chaque patrimoine dont la gestion a été confiée au Trésor Public.

******

Pour atteindre cet objectif, la Direction Générale de la Comptabilité Publique adopte une **politique générale de sécurité du système d'information (PGSSI)** dont les principales dispositions, énoncées dans le présent document, visent à préciser les lois, règlements et pratiques qui régissent la façon de gérer et protéger le SI du Trésor Public.

Cette politique est conforme au plan de renforcement de la sécurité des SI de l'Etat élaboré par les services du Premier Ministre. Elle respecte les principes de la politique de sécurité interne du MinEFI (organisation et responsabilités, intégration de la sécurité dans les projets, principes de contrôle, sensibilisation et formation…) élaborée par le Haut Fonctionnaire de Défense. La méthodologie retenue pour son élaboration est celle proposée par la Direction centrale pour la sécurité des systèmes d'information et tient compte des thèmes définis par la norme ISO 17799.

******

Afin que les actions de sécurité du SI découlent de la même interprétation des objectifs et que les informations soient exploitées et échangées au sein du Trésor Public et avec les partenaires dans des conditions cohérentes et compatibles de sécurité, la PGSSI s'applique à compter de sa publication :

- à la Direction Générale de la Comptabilité Publique et aux services déconcentrés ;
- à l'ensemble des agents, titulaires ou non, autorisés à accéder aux ressources composant le SI du Trésor Public ;
- contractuellement, ou par le biais de conventions, aux usagers, partenaires et fournisseurs, dès lors qu'ils accèdent au SI du Trésor Public ou que leur propre SI y est relié.

La PGSSI couvre :

- l'ensemble des processus, procédures et ressources informatiques et de télécommunication (systèmes d'exploitation, serveurs, éléments réseaux, terminaux, applications, données…) destinés à élaborer, traiter, stocker, acheminer, présenter ou détruire des informations, quelle que soit leur forme matérielle ou immatérielle (support papier, support électronique) ;
- les environnements d'exploitation (bâtiments et locaux hébergeant les ressources informatiques et de télécommunication du Trésor Public).

1. Exigences de sécurité

Sans que cette liste soit exhaustive, les exigences *(cf. définitions au § 2.1)* développées ci-après constituent autant de domaines de préoccupation auxquels une attention particulière doit être apportée :

- un besoin relativement fort de disponibilité du SI aux échéances, majoritairement pour le recouvrement de l'impôt et le règlement des paies et pensions. L'emploi des nouveaux canaux de communication renforce cette exigence. Enfin, le « paiement en aveugle » est difficile en raison des volumes traités et de la forte disparité des bénéficiaires et des montants ;
- un besoin fort en intégrité des données et des traitements, pour l'exactitude des opérations (payer/recouvrer auprès du bon acteur), pour le pilotage des activités (comptabilité, statistiques), pour les informations restituées par les nouveaux canaux ;
- un besoin de confidentialité pour le traitement de données à caractère personnel internes et externes (exigences de la CNIL), pour les informations internes ou confiées par des tiers et soumises à une obligation légale ou réglementaire de confidentialité (secret défense, secret fiscal, secret douanier, secret statistique…), et pour toute autre information dont la divulgation aurait des conséquences graves pour l'Etat ou pour des tiers (cas des marchés sensibles par exemple) ;
- un besoin constant d'éléments de preuve et de contrôle dans les applications métiers (pistes d'audit, imputabilité des opérations à leurs auteurs…) pour l'investigation en cas de dysfonctionnements ou d'incidents, et pour faciliter les activités de contrôle interne et d'audit. Les conditions d'enregistrement, de traitement et de conservation des informations doivent permettre une reconstitution aisée des opérations effectuées dans le cadre des activités du Trésor Public et une justification de l'existence des informations ;
- un besoin relativement faible en garantie d'anonymat en dehors de quelques applications qui viennent en support de la gestion du personnel et des outils de simulation offerts aux internautes.

Le respect de ces exigences conditionne l'efficacité interne du Trésor Public et le maintien de la confiance des parties prenantes (autorités de tutelle, usagers, partenaires…) dans sa capacité à respecter ses engagements, assurer ses missions et maîtriser toute situation de risque majeur susceptible de provoquer notamment :

- une réserve dans le cadre de la certification des comptes ;
- un retard dans la mise à disposition des fonds d'intervention à caractère social ;
- une désorganisation interne qui proviendrait d'une augmentation non maîtrisable des dossiers à instruire en mode dégradé ou de l'accueil physique dans les services déconcentrés ;
- des pertes de trésorerie générée par un retard dans les processus de recouvrement et d'encaissement ;
- le paiement d'intérêts moratoires générés par un retard dans le règlement des fournisseurs de l'Etat ;
- la génération d'indus entraînant une perte financière indirecte due à la charge de traitement a posteriori ;
- des pertes financières dues à des fraudes internes ou externes, toute fraude étant inacceptable quel qu'en soit son montant ;
- la mise en cause de la responsabilité d'un agent.

2. Principes directeurs de la PGSSI

La PGSSI est fondée sur la satisfaction des neuf principes fondamentaux développés ci-après :

- classification des ressources ;
- approche raisonnée de la sécurité du SI ;
- organisation autour de la sécurité du SI claire et opérante ;
- intégration de la sécurité du SI dans les projets ;
- maîtrise des accès au SI ;
- garantie de la continuité des activités ;
- capacité de réaction à incident ;
- sensibilisation et formation ;
- visibilité permanente.

2.1 Classification des ressources

Toute démarche en matière de sécurité du SI a pour objectif la création, dans la mesure du possible, de « périmètres de confiance » délimités et maîtrisés aux plans réglementaire, organisationnel, technique et humain.

Il s'agit donc de déterminer ces périmètres (domaine d'activité, processus de gestion, activité, application…), qui d'ailleurs pourront s'étendre progressivement, d'inventorier les ressources du SI qui les supportent en précisant l'usage qui en est fait, de désigner leurs propriétaires puis de les classifier selon leur sensibilité.

La sensibilité des ressources est déduite des niveaux d'exigence de sécurité exprimés par les propriétaires et étayés par les impacts des situations de risque susceptibles de remettre en cause le respect d'une exigence.

Les normes retenues par le Trésor Public pour classifier les ressources sont de cinq natures :

- disponibilité (attribut D) : le SI doit garantir l'exécution des contrats et des obligations correspondantes, ainsi que la disponibilité des informations dans des conditions prédéfinies d'horaire, de délai et de performance ;
- intégrité (attribut I) : le SI doit assurer que les informations administratives, comptables et financières sont inaltérables dans le temps et dans l'espace, et garantir leur exhaustivité, leur validité et leur cohérence ;
- confidentialité (attribut C) : le SI doit assurer le maintien du secret des informations sensibles stockées et échangées et réserver leur accès à des personnes dûment autorisées ;
- « possibilité de preuve et contrôle » (attribut P) : le SI doit répondre au mieux aux exigences réglementaires et juridiques et aux principes de contrôle interne à travers trois mécanismes complémentaires qui sont la trace, l'imputation et la non répudiation ;
- anonymat des acteurs (attribut A) : disposition par laquelle une personne créant une information et/ou effectuant une action qui fait l'objet d'un traitement informatique ne puisse être identifiée directement ou indirectement.

2.2 Approche raisonnée

Seul un équilibre entre une « prise de risque calculée » et le « coût de la sécurité » est viable. C'est pourquoi, les plans d'action sécurité doivent répondre aux objectifs suivants :

- éliminer les risques inacceptables (remettant en cause les intérêts fondamentaux de l'Etat ou des tiers) ;
- en cas d'arbitrage, mettre en perspective les incidences financières potentielles des situations de risque craintes avec le coût des mesures de sécurité du SI ;
- surveiller les risques acceptés pour s'assurer qu'ils restent à un niveau acceptable.

L'appréciation des risques repose sur :

- l'évaluation des impacts potentiels des risques les plus craints (risque brut) ;
- l'appréciation de la capacité de l'organisation à se protéger et à réagir (niveau de maîtrise des risques) ;
- le calcul de l'occurrence potentielle des risques (fréquence des événements) ;
- la pondération des impacts potentiels par la capacité de l'organisation à se protéger et par la fréquence des événements (risque net) ;
- la définition d'un niveau de risque acceptable.

Les plans d'action sécurité visent à rapprocher le risque net du niveau de risque acceptable.

Pour estimer la potentialité des risques liés au SI, il est impératif de recenser les incidents rencontrés et leurs impacts afin de disposer d'une « base d'expérience », dans la logique des approches menées sur la surveillance des risques.

2.3 Organisation claire et opérante

L'organisation de la sécurité du SI a pour but de maintenir un niveau de sécurité conforme aux enjeux et à la stratégie du Trésor Public. Elle respecte trois lignes directrices:

- l'organisation est fondée sur la responsabilité adaptée à chaque contexte et s'appuie, dans la mesure du possible, sur les structures en place dans un souci d'économie et de performance. Elle couvre un ensemble de missions assurées :
  - au sein d'une «filière» (chaîne fonctionnelle) dédiée à la sécurité du SI, par des acteurs à qui des missions afférentes à ce domaine de préoccupation ont été confiées (cf. § 3.2),
  - au sein de la Direction Générale de la Comptabilité Publique et des services déconcentrés, au plus près des opérations, par l'ensemble des collaborateurs en fonction de leur niveau de responsabilité (cf. § 3.1),
  - par les corps de contrôle qui vérifient le respect de la PGSSI et de ses documents d'application (cf. § 3.3),
  - par des instances transverses de pilotage qui s'assurent du traitement des menaces majeures et procèdent aux arbitrages (cf. § 3.4) ;
- l'organisation est efficiente et repose sur trois types de missions :
  - le pilotage de la sécurité du SI qui suit la mise en application de la PGSSI et s'assure de l'adéquation entre les dispositions prises et les objectifs fixés,
  - le support qui fournit les moyens (outils méthodologiques, bases de connaissances, supports de sensibilisation…) requis à la réalisation des tâches opérationnelles et de contrôle,
  - l'opérationnel qui couvre la mise en application de la PGSSI (expression des besoins, administration des moyens, sensibilisation, surveillance, audit…) ;
- l'organisation respecte le principe de séparation des pouvoirs et distingue, aussi bien en mode projet qu'en fonctionnement opérationnel, six types de mission :
  - la définition du besoin de sécurité et l'arbitrage relevant des sous-directions, relayées par leurs maîtrises d'ouvrage et par les propriétaires de ressources,
  - la conception et le développement des solutions de sécurité du SI relevant de la Sous-direction du système d'information relayée par les maîtrises d'œuvre de développement,
  - l'intégration des solutions de sécurité du SI relevant de la Sous-direction du système d'information relayée par les maîtrises d'œuvre d'intégration,
  - l'exploitation des solutions de sécurité du SI relevant de la Sous-direction du système d'information relayée par les exploitants,
  - la surveillance et le contrôle intégrés aux organisations et assumés par chaque collaborateur ou par des structures dédiées,
  - l'audit relevant de la MAEC et l'inspection du corps des inspecteurs principaux, appuyés par des experts indépendants des entités contrôlées, répondant à des règles déontologiques précises et respectant des protocoles adaptés.

2.4 Maîtrise des accès au SI

La maîtrise des accès au SI du Trésor Public repose sur le respect de quatre exigences :

- toute personne ayant besoin d'accéder au système d'information doit se voir attribuer explicitement des droits d'accès personnels lui permettant d'exercer uniquement les fonctions nécessaires à son activité professionnelle ;
- tout changement, ou cessation d'activité, même temporaire, doit entraîner systématiquement une révision ou une révocation de ces droits d'accès ;
- l'attribution de ces droits est de la seule responsabilité des propriétaires des ressources du SI, ce processus pouvant être délégué sous le couvert d'un contrôle ;
- tout droit d'accès au SI doit pouvoir être justifié et contrôlé en permanence, notamment par les responsables hiérarchiques et les administrateurs.

Le respect de ces exigences suppose la mise en œuvre de trois dispositifs complémentaires :

- le contrôle des accès logiques qui repose sur quatre concepts, déclinés sur les plans organisationnel et technique selon l'environnement contrôlé : l'identification, l'authentification, l'habilitation et l'autorisation ;
- le cloisonnement des réseaux qui vise à contrôler globalement les accès et à contenir d'éventuels incidents de sécurité en limitant leur propagation. Il implique que l'architecture soit formalisée, que les points d'accès vers l'extérieur soient identifiés, que le réseau soit structuré en domaines de confiance placés sous une autorité unique et que les règles de communication entre domaines soient établies ;
- la traçabilité qui permet de reconstituer tout ou partie des actions d'un utilisateur et des actions d'administration du SI, ou de comprendre a posteriori le fonctionnement du SI. Elle s'appuie sur les mécanismes de contrôle d'accès et de cloisonnement qui génèrent des traces au niveau de l'infrastructure, mais aussi sur les applications elles-mêmes qui fournissent des pistes d'audit en regard de la logique des métiers.

2.5 Garantie de continuité des activités

Le Trésor Public doit être en mesure de répondre à des événements imprévus susceptibles de rendre indisponible tout ou partie de son SI et, ainsi, préserver la continuité des services offerts aux usagers et partenaires. Aussi, pour chaque processus métier, doivent être formalisés :

- les plans de continuité prévus (solutions de secours, modes dégradés possibles, sites de repli…) en regard des scénarios de risques physiques et logiques craints et des enjeux en termes de perte de données et d'interruption du service ;
- les pré-requis aux plans de continuité (sauvegardes de recours, astreintes…) ;
- l'organisation permettant la prise en compte effective des alertes et des incidents ou dysfonctionnements graves en minimisant leurs impacts *(cf. § 2.7)* ;
- les conditions de test et d'actualisation des procédures de reprise et de secours ;
- les processus d'audit des dispositifs prévus.

2.6 Intégration de la sécurité du SI dans les projets

Plus elle est appréhendée tôt, plus la sécurité est efficace et moins elle est coûteuse. La sécurité du SI doit systématiquement être prise en compte tout au long du cycle de vie des projets et aboutir à la mise en œuvre de fonctions de sécurité adéquates dans le respect de trois exigences :

- cohérence : la sécurité d'un système est toujours celle du composant le plus faible. Les fonctions de sécurité doivent fournir un niveau homogène et cohérent sur l'ensemble du SI dans tous les domaines de la prévention (exposition, dissuasion, robustesse) et de la réaction (détection et mesures d'urgence, palliation, réparation) ;
- intégration : les fonctions de sécurité doivent s'appuyer, dans la mesure du possible, sur les moyens organisationnels et techniques existants. Elles doivent être mises en oeuvre en veillant à l'adhésion de tous les acteurs impliqués ;

- efficacité : les règles et services de sécurité doivent trouver une mise en application aisée au travers de technologies si possible éprouvées et de procédures simples.

Une démarche spécifique d'intégration de la sécurité dans les projets (démarche ISP) fournit les supports permettant aux acteurs de prendre en compte la sécurité du SI et de compléter la documentation nécessaire à la compréhension et au contrôle du SI en conservant, notamment, une trace des arbitrages effectués. Elle doit être utilisée pour les nouveaux projets ; elle permet également de documenter a posteriori les projets déjà engagés et les systèmes opérationnels.

2.7 Capacité de réaction à incident

Devant la diversité des menaces d'origine naturelle, accidentelle ou criminelle qui pèsent sur son SI, le Trésor Public doit mettre en place à tous les niveaux :

- des dispositifs de veille dont l'objet est d'anticiper les scénarios de risques liés au SI (nouvelles menaces et nouvelles vulnérabilités) et de réduire le nombre d'incidents ;
- des processus et procédures de surveillance et de réaction dont l'objet est de détecter au plus tôt les incidents de sécurité du SI inévitables et de minimiser leurs impacts dans le cadre d'une réponse coordonnée à l'échelle du Trésor Public.

Chaque dispositif précisera :

- les principes d'organisation (cellules de crise décisionnelle et opérationnelles, porte-parole externe et interne…), en respectant les responsabilités définies au chapitre 3 ;
- les circuits de communication des informations entre les sous-directions et les services déconcentrés ;
- la « logique d'escalade » correspondant au niveau d'alerte ou de sévérité retenu.

2.8 Sensibilisation et formation des agents

L'efficacité des dispositifs de sécurité du SI repose le plus souvent sur l'utilisation qui en est faite et sur le respect des valeurs éthiques et déontologiques. C'est pourquoi la sensibilisation et la formation des agents à la sécurité du SI sont des actions prioritaires. Tournées vers la responsabilisation des acteurs, elles contribuent significativement à la réduction des risques encourus quand elles identifient le facteur humain à la fois comme élément de risque potentiel (erreurs, négligences, déviances) et comme moyen de protection (meilleures pratiques, actualisation des connaissances relatives aux menaces, acquisition des réflexes de vigilance, amélioration de la capacité de réaction à incident).

La sensibilisation et la formation doivent être illustrées par des exemples concrets, être adaptées à chaque contexte métier et à chaque environnement culturel, et s'intégrer dans une logique visant à assurer une cohérence d'ensemble.

En ce qui concerne les usagers et les partenaires, les sous-directions établiront, en regard des services offerts et de leur sensibilité, des campagnes d'information sous forme de recommandations ou de guides pratiques en s'appuyant sur le Service communication et sur la Mission sécurité du SI.

2.9 Visibilité permanente

Une organisation de suivi et de contrôle doit être définie afin de disposer d'une visibilité sur l'évolution des risques liés au SI et sur les niveaux de protection atteints qui doivent être périodiquement appréciés.

Un dispositif de tableaux de bord (stratégiques, de pilotage et opérationnels), géré par la Mission sécurité du SI, doit permettre de suivre :

- le niveau d'application des règles de sécurité du SI édictées ;
- les menaces qui pèsent sur le SI du Trésor Public ;
- le niveau de sécurité atteint en regard des vulnérabilités du SI et les risques résiduels ;
- les incidents avérés et leurs impacts ;
- la mesure de l'effort déployé pour la sécurité du SI et l'efficacité des plans d'action.

Les indicateurs majeurs mettant en perspective l'évolution de la sécurité du SI doivent faire l'objet d'une présentation régulière au Directeur Général de la Comptabilité Publique.

3. Responsabilités

Dans un souci de cohérence et en conformité avec les règles de délégation, les principes de responsabilité développés ci-après doivent être respectés.

3.1 Direction Générale de la Comptabilité Publique et services déconcentrés

La **Direction Générale** veille à ce que la sécurité du SI soit adaptée aux risques réels et aux enjeux (impact du risque, coût des parades). Elle s'assure que chaque sous-direction a déterminé les niveaux de risque acceptables et que les procédures de continuité des activités sont testées et suffisantes pour respecter les engagements pris vis-à-vis de l'Etat, des tiers et des agents.

Les **sous-directions métiers et fonctionnelles** déterminent le risque maximum acceptable de chaque activité dont elles ont la charge. En s'appuyant sur leurs maîtrises d'ouvrage et les propriétaires des ressources qu'elles auront désignés, elles inventorient et classifient ce qu'il est nécessaire de protéger et à quel niveau, et expriment leurs besoins en matière de sécurité. Elles informent le plus rapidement possible la Direction Générale et l'AQ-SSI en cas de situation de risque fort pour l'une des parties prenantes.

La sécurité est d'autant plus efficace qu'elle est décentralisée au niveau le plus proche des événements et des acteurs. C'est pourquoi chaque **Trésorier Payeur Général** intègre les règles relatives à la sécurité du SI dans ses processus de gestion, sensibilise à la sécurité du SI l'ensemble du personnel qui lui est rattaché et, selon les procédures prévues, remonte aux acteurs en charge de la sécurité du SI (correspondants, responsables de la sécurité du SI, AQ-SSI) les incidents de sécurité majeurs.

Toute ressource (processus, infrastructures, équipement, programmes et données), pour chaque domaine fonctionnel ou technique, est placée sous le contrôle d'un **propriétaire**. Celui-ci doit tenir un inventaire, déterminer le « profil de sécurité » (exigences en termes de disponibilité, intégrité, confidentialité, preuve et contrôle, anonymat) et les règles de gestion de chaque ressource, et conduire les analyses de risque en relation avec la Mission sécurité du SI.

L'**encadrement de proximité**, qui adopte un comportement ayant valeur d'exemple, respecte et fait respecter les lois et règlements tant par le personnel qui lui est rattaché que par celui des sous-traitants auxquels il fait appel. Il exerce un contrôle permanent et informe les correspondants sécurité de toute situation anormale tout en sauvegardant les éléments de preuve de l'anomalie.

Chaque **utilisateur** doit respecter les règles de sécurité portées à sa connaissance, ne pas contourner les dispositifs de sécurité mis en place et informer sa hiérarchie et son correspondant sécurité de tout incident ou anomalie constatée.

La **Sous-direction système d'information** assure le développement du SI et le bon fonctionnement des ressources informatiques et de télécommunication dont elle est dépositaire. A ce titre, il est de sa responsabilité de concevoir et mettre en oeuvre les services de sécurité et de contrôle répondant aux exigences convenues avec les sous-directions et permettant de détecter et limiter tout incident ou toute anomalie (tentatives d'accès non autorisé, indisponibilité d'une ressources, code malveillant…).

La **Sous-direction ressources humaines** tient compte dans ses missions - de supervision, de coordination, de veille et de conseil - des aspects législatifs, réglementaires et déontologiques ayant trait à la sécurité du SI. Elle fournit les informations permettant à chaque collaborateur d'exercer ses responsabilités et s'assure de l'adéquation entre les dispositifs prévus et les obligations juridiques et réglementaires qui doivent être respectées.

Les **directeurs de programme et les chefs de projets** fournissent aux acteurs des projets les moyens permettant la prise en compte effective de la sécurité du SI et gèrent formellement les arbitrages susceptibles de générer des risques majeurs pour l'Etat, le Trésor Public, les tiers et les agents, qu'ils communiquent à l'AQ-SSI. Ils peuvent s'appuyer, autant que de besoin, sur les acteurs de la filière sécurité du SI.

Les **maîtrises d'ouvrage** (MOA), représentant les sous-directions, expriment dans le cadre des projets un niveau de sécurité acceptable au regard d'une évaluation des risques. Elles s'appuient sur les compétences des acteurs de la filière sécurité du SI et les outils méthodologiques mis à leur disposition. Elles s'assurent de la conformité des livrables (respect des exigences de sécurité, scénarios de recette, documentation utilisateur, documentation des processus) et accompagnent la mise en place des solutions développées ou acquises. Elles signalent à leur hiérarchie et à la Mission sécurité du SI les arbitrages susceptibles de générer de nouveaux risques.

Les **maîtrises d'œuvre**, au regard de l'expression du niveau de sécurité requis, étudient les parades possibles et spécifient et développent les services de sécurité qu'elles font valider par les MOA. Elles contribuent à la rédaction des clauses contractuelles concernant les exigences de sécurité envers les prestataires et partenaires techniques.

Les **exploitants** (départements informatiques, centres d'encaissement, gestionnaire du service messagerie…) s'assurent que les nouvelles applications mises en production sont compatibles avec les environnements de production et ne génèrent pas de nouveaux risques. Ils assurent le maintien à niveau des configurations de sécurité et le maintien en condition opérationnelle des dispositifs de secours. Ils participent à la cartographie des ressources et à leur classification.

3.2 Filière sécurité du SI en support

Par délégation du Directeur Général, l'**Autorité Qualifiée de la Sécurité du SI** (AQ-SSI), responsable de la Mission sécurité du SI, élabore la PGSSI et veille à son application. L'AQ-SSI fait établir et renouveler régulièrement par les sous-directions et les services déconcentrés les analyses de risques liés au SI, et veille au traitement des risques jugés inacceptables. L'AQ-SSI vérifie que les orientations prises dans le cadre des programmes et projets n'ont pas de conséquences préjudiciables pour les différentes parties prenantes (Etat, ministères, autres directions du MinEFI, tiers…). Il informe régulièrement le Directeur Général, le Sous directeur du système d'information et la MAEC de l'évolution des risques liés au SI et du niveau de sécurité atteint.

Les **responsables de la sécurité du système d'information** (RSSI) maintiennent une vision permanente des risques afférents aux infrastructures de production informatique du Trésor Public. Ils s'assurent du déploiement et du maintien en condition opérationnelle des solutions et services de sécurité requis à la protection des infrastructures dont leur entité est dépositaire. Ils participent à l'élaboration des volets sécurité des dossiers de mise en production et valident la compatibilité des solutions de sécurité retenues avec les contextes d'exploitation. Ils contribuent, en particulier, au choix et à la mise en œuvre des solutions de secours. Les RSSI effectuent un reporting auprès de leur hiérarchie et de l'AQ-SSI qu'ils alertent en cas de situation de risque majeur.

Suivant les besoins, des fonctions de **correspondants de sécurité des SI** (CSSI) sont mises en place au sein des entités opérationnelles. Les CSSI réalisent la mise en conformité de leur entité avec la PGSSI et délivrent conseil et assistance au quotidien et au cours des projets. Ils contribuent à la surveillance permanente des menaces et des vulnérabilités et remontent les incidents de sécurité à leur hiérarchie et à l'AQ-SSI. En fonction du périmètre dans lequel ils évoluent et de leurs domaines de compétence, ils peuvent être amenés à réaliser des missions complémentaires (assistance aux directeurs de programmes et aux chefs de projets, assistance aux maîtrises d'ouvrage et d'œuvre, support aux exploitants).

Le **Site National de Sécurité** (SNS) participe à la définition et la mise en place des plans et solutions de secours d'exploitation, qu'il peut être amené à exploiter. A la demande de l'AQ-SSI, il est amené à réaliser des études ou à développer certains dispositifs de sécurité.

3.3 Corps de contrôle

La **MAEC** et les **auditeurs du réseau du Trésor Public**, réalisent ou supervisent les audits et enquêtes relatives à la sécurité du SI en s'appuyant sur les experts requis, à condition que ces derniers ne fassent pas partie de l'entité auditée. Les auditeurs s'assurent du respect des règles de sécurité édictées, évaluent en permanence la qualité des dispositifs de prévention et réaction déployés au sein des sous-directions et des services déconcentrés, et suivent la mise en œuvre des recommandations formulées. A ce titre, ils vérifient que les dispositifs de contrôle interne de

chaque entité prennent en compte la surveillance des risques liés au SI. Les auditeurs et inspecteurs doivent respecter des protocoles spécifiques afin de limiter les risques inhérents à ce type d'intervention.

3.4 Instances de pilotage

le **Costrat-GSI**, sur proposition de l'AQ-SSI, inscrit à son ordre du jour la sécurité du SI. Il définit le cadre général dans lequel s'inscrit la PGSSI et ses documents d'application, coordonne les actions de sécurité transverses et procède aux arbitrages majeurs relatifs à la sécurité du SI.

Le **Comité de pilotage de la sécurité du SI** (Copil-SSI) se réunit sur convocation de l'AQ-SSI ou à l'initiative d'un des membres permanents. Son fonctionnement est fondé sur un travail participatif visant essentiellement à commenter et valider les travaux relatifs à la sécurité du SI. Ses membres permanents sont l'AQ-SSI, qui anime le Copil-SSI, les RSSI, un représentant de la MAEC, un représentant de la Sous-direction pilotage réseaux et moyens et le responsable du SNS.

Deux fois par an, il aborde les projets majeurs consacrés à la sécurité du SI et aux plans de secours en présence du Sous-directeur du système d'information et du TPG dont dépend le SNS.

Une fois par an, il est étendu à l'ensemble des acteurs de la filière SI, afin de faire le point sur la mise en œuvre des actions sécurité et sur les programmes / projets.

Pilotage des programmes et des projets : dans le cadre des programmes et projets majeurs dans lesquels est impliqué le Trésor Public, chaque directeur de programme / projet définit explicitement les principes de gouvernance de la sécurité du SI. Il intègre au sein des instances de pilotage des projets les éléments permettant la prise en compte effective de la sécurité du SI et crée, si nécessaire, une structure de pilotage ou de suivi dédiée.

Coordination au sein du MinEFI : tous les deux mois, le Fonctionnaire de la Sécurité du Système d'Information (FSSI) du MinEFI réunit l'ensemble des AQ-SSI pour suivre les projets transverses et rechercher les mutualisations possibles.

4. Obligations liées au SI

4.1 Cadre législatif et réglementaire

Le Trésor Public est soumis à des obligations légales, réglementaires, contractuelles et, en tant que personne morale, doit s'assurer tout particulièrement que :

- ses activités se déroulent conformément aux lois et règlements (français et européens) ;
- suite à une opération présentant un caractère illicite, il a la capacité de fournir les éléments de preuve relatifs à un traitement informatique.

Les agents doivent respecter la législation applicable en France et, le cas échéant, à l'étranger, notamment en matière de protection des données nominatives, propriété intellectuelle, fraude informatique, cryptologie, protection de la vie privée et secret des correspondances.

La liste des textes de références est tenue à jour et accessible sur l'Intranet sécurité.

4.2 Comportements et règles de conduite

Les comportements et règles de conduite relatives à la sécurité du SI doivent être identifiés, formalisés et communiqués à l'ensemble des agents et prestataires par le biais de différents vecteurs (code de déontologie, charte d'utilisation des Technologies de l'Information et de la Communication, règlements intérieurs…) précisant les obligations (loyauté, discrétion, respect du secret professionnel…), interdictions et procédures à appliquer dans l'accomplissement des missions. Ils visent à réaliser un équilibre entre les besoins de sécurité et le respect des libertés individuelles et collectives, et instaurer un bon usage des TIC.

4.3 Contrats de prestations et conventions de services

Les contrats de prestation et les conventions de services touchant à des tâches jugées « sensibles » doivent faire l'objet de contrôles et nécessitent des dispositions particulières relatives à la protection des actifs du Trésor Public. Sont notamment visées :

- toutes les prestations intellectuelles concernant de près ou de loin la sécurité du SI, son audit ou son contrôle ;
- les prestations d'infogérance ou de sous-traitance qui nécessitent des dispositions particulières pour délimiter la responsabilité des contractants, assurer la confidentialité des informations sensibles et organiser le contrôle des mesures de sécurité déployées.

Par ailleurs, pour être raccordée au SI du Trésor Public, une entité externe, quelle qu'elle soit (autre administration, partenaires, sous-traitant…), doit respecter des règles de sécurité contractuellement définies (périmètre de connexion au SI du Trésor Public, responsabilités respectives, référentiel de sécurité appliqué…).

Aussi, appartient-il aux signataires des contrats de sous-traitance ou d'infogérance de prendre les dispositions contractuelles nécessaires à la prise en compte de la présente politique en faisant appel, si nécessaire, aux experts en la matière (AQ-SSI, RSSI, juriste, informaticiens…) et de prévoir les procédures d'audit adéquates.

Enfin, pour toutes les fournitures et services achetés ayant une incidence sur la sécurité, il ne sera fait appel qu'à des fournisseurs méritant une confiance en rapport avec cette incidence.

5. Mise en œuvre de la PGSSI

5.1 Déclinaison opérationnelle

La déclinaison de la PGSSI se traduit formellement par un cadre structuré appelé « cadre de référence de la sécurité du SI» qui s'articule autour de deux types de documents :

- les instructions et notes de service relatives à la sécurité du SI : elles sont opposables par la MAEC. Elles précisent le cadre réglementaire par axe de sécurité et peuvent se traduire, au cas par cas, par des engagements de responsabilité. Elles sont proposées par les sous-directions, validées et référencées par l'AQ-SSI et visées, après concertation des parties prenantes, du Directeur Général ;
- les guides opérationnels (méthodes, préconisations techniques, référentiels de contrôle interne et d'audit, guides comportementaux…) : ils favorisent un déploiement cohérent des dispositifs de sécurité, le développement de la culture sécuritaire du Trésor Public et une approche économique de la sécurité du SI. Ils émanent des acteurs de la filière sécurité et sont validés et référencés par l'AQ-SSI.

5.2 Suivi et contrôle

5.2.1 Évolution de la PGSSI

La PGSSI a vocation à être un document stable dans le temps. Cependant, elle doit tenir compte des changements qui peuvent affecter le SI et son environnement et doit être mise à jour en fonction d'événements internes tels que la mise à jour des plans stratégiques du Trésor Public ou de son organisation ou d'événements externes tels que le changement de la législation et du cadre réglementaire de la fonction publique, la publication de nouvelles normes nationales, européennes ou internationales et l'apparition de nouvelles menaces.

L'évolution de la PGSSI est placée sous l'autorité de l'AQ-SSI qui propose au Directeur Général, en s'appuyant sur le Costrat-GSI, les révisions et versions successives.

5.2.2 Diffusion du document de PGSSI

Destinée à être connue, la PGSSI ne fait pas l'objet de protection particulière et a vocation à être communiquée.

5.2.3 Évaluation de la PGSSI

5.2.3.1 Rapports périodiques

Le Copil-SSI, sous la conduite de l'AQ-SSI, élabore une fois par an un rapport destiné au Costrat-GSI sur la sécurité du SI. Ce rapport évalue notamment le niveau d'application de la PGSSI. Ce rapport permet aux membres du Costrat-GSI d'une part, d'apprécier l'état de la sécurité du SI et, d'autre part, d'en rendre compte aux autorités de tutelle.

5.2.3.2 Audits de sécurité du SI

L'AQ-SSI est informé par la MAEC des programmes annuels prévisionnels des audits de sécurité et peut proposer de les compléter. Il contribue à la validation des protocoles utilisés dans le cadre de ces audits afin de limiter les risques associés (objectifs, lettre de mission, procédure à suivre, supports, nature des engagements, livrables, procédure en cas de découvertes d'anomalies).

5.2.3.3 Traitement des cas de non-respect

Les cas de non-respect de la PGSSI, quelle qu'en soit leur cause (impossibilité technique, législation locale, arbitrage économique, erreur, malveillance), doivent être signalés à la hiérarchie et à l'AQ-SSI, avec indication des mesures prises pour limiter les conséquences de ces situations ou éviter qu'elles ne se reproduisent. Un suivi spécifique de ces cas doit être mis en place.

6. Articulation de la PGSSI

Pour préserver une certaine cohérence et efficacité aux dispositifs de surveillance des risques, les dispositions prises en matière de sécurité du SI doivent principalement s'articuler avec :

- les **dispositions prises en matière de contrôle interne** (définition d'objectifs partagés, mise en commun des outils et référents, articulation des activités de surveillance et de contrôle des risques...) ;
- les **dispositions prises en matière de continuité des activités** (mise en conformité des plans de secours et de continuité, articulation des dispositifs d'alerte et de réaction avec les dispositifs de gestion de crise, sécurisation des processus de secours…) ;
- les **dispositions prises en matière de sécurité des personnes et des biens** (mise en conformité des mesures de protection des sites et des bâtiments avec les exigences de protection du SI : sécurité des accès physiques, sécurité incendie, protection contre le dégât des eaux, climatisation, sécurité des alimentations électriques…) ;
- les **dispositions prises en matière de contrôle de conformité** (déclinaison commune des règles et des normes relatives à la sécurité du SI, identification des processus de contrôles réguliers, élaboration conjointe de tableaux de bord) ;
- les **dispositions prises en matière d'urbanisation** du SI (intégration des services de sécurité dans les différentes cibles d'urbanisation, communication des cartographies de processus ou d'applications, prise en compte de la sécurité dans les règles et principes d'urbanisme….).

Par ailleurs, tout **programme ou projet d'importance** au sein du MinEFI et concernant le Trésor Public doit prendre en compte la présente politique, faire l'objet d'une documentation relative à la sécurité (notes de synthèse, dossiers sécurité, livrables spécifiques…) et s'inscrire dans un cadre qui précise :

- les engagements entre les parties prenantes du programme / projet et leurs relations ;
- les indicateurs permettant à chacun d'avoir une visibilité permanente sur l'avancement du programme et le niveau de sécurité atteint en regard des exigences de sécurité requises ;
- la procédure d'alerte en cas de situation remettant en cause l'atteinte d'un objectif projet ou le respect d'une exigence majeure de sécurité.