Direction Système d'Information GRDF
Cybersécurité

www.grdf.fr

N° 23-TPIT-088

Prestation Gouvernance et Risques

DESCRIPTIF DES PRESTATIONS

Appel à candidatures

- **DATE :** 05/06/2023
- **VERSION :** 1.0
- **AUTEURS :** ADRIEN LUTFALLA, YANN CADORET
- **DESTINATAIRES :** SECOIA

Table des matières

1 Objet de la consultation

1.1 Contexte & objectifs de la consultation

La présente consultation a pour objectif de proposer des prestations relatives à la gouvernance et à la gestion des risques cybersécurité de GRDF.

GRDF souhaite se faire accompagner sur 5 prestations réparties en 3 lots.

Lots	Prestations	Description
Lot 1 : Gouvernance	**Mise en place d'un SMSI**	Accompagnement de GRDF dans la finalisation de son Système de Management de la Sécurité de l'Information et la mise en place des processus de surveillance et des actions d'amélioration continue.
	Certifications / Conformités / Evaluation de la maturité	Réalisation d'évaluations et d'analyse d'écart interne sur divers périmètres GRDF (). Analyse ponctuelle d'éléments cybersécurité réglementaires et normatifs.
	Pilotage	Accompagnement de GRDF dans le suivi des différents plans d'action cybersécurité et dans l'assistance à la chefferie de projets cybersécurité sur des projets de gouvernance, risque et conformité cybersécurité.
Lot 2 : Gestion stratégique des risques	**Gestion des risques au niveau stratégique**	Soutien à la gestion des risques stratégiques cybersécurité avec la réalisation d'analyses de risques macro (processus d'entreprise), la définition du programme d'audit ou encore l'accompagnement au pilotage des risques et des indicateurs.
Lot 3 : Gestion opérationnelle des risques	**Gestion des risques au niveau opérationnel**	Accompagnement à l'homologation des systèmes en suivant la Politique d'Homologation de GRDF. Réalisation d'Analyses de Risques cybersécurité dans le cadre des projets d'homologations.

Les différentes prestations pourraient être réalisées en plusieurs temps :

- dans un premier temps, il est demandé au Titulaire de mettre en place les différents processus et de formaliser la documentation ;
- dans un second temps, le Titulaire devra réaliser les actions formalisées (ex : amélioration continue du SMSI, évaluation de la sécurité, analyse de risques sécurité dans le cadre d'une homologation, etc.).

1.2 Terminologie et glossaire

Dans le présent cahier des charges, GRDF sera désigné par « le Client ».

Il est convenu de nommer « Titulaire » le titulaire contractant du marché suivant le lot concerné et il est convenu de nommer « Soumissionnaire » les entreprises répondant à la consultation.

Pour l'interprétation du présent cahier des charges, les termes suivants commençant par une majuscule, employés indifféremment au singulier ou au pluriel, auront la signification qui leur est attribuée ci-après :

Délai d'intervention : le délai d'intervention d'un geste de proximité est défini comme le temps écoulé entre la demande de GRDF et le début de la réalisation du geste technique concerné par l'hébergeur.

Délai d'exécution : le délai d'exécution d'un geste de proximité est défini comme le temps écoulé entre la demande de GRDF et la réalisation effective et conforme du geste technique demandé.

« Informations Commercialement Sensibles (ICS) »: désigne toute information qui entre dans le champ de l'article R.111-31 du Code de l'énergie relatif à la confidentialité des informations détenues par les opérateurs exploitant des ouvrages de transport, de distribution ou de stockage de gaz naturel ou des installations de gaz naturel liquéfié, à savoir : 1° les dispositions des contrats et protocoles ayant pour objet l'accès aux ouvrages et aux installations, y compris celles fournissant des services auxiliaires, l'utilisation des stockages, le transit ou les achats conclus en vue de l'équilibrage des réseaux ainsi que les informations échangées pour la préparation et l'application des contrats et protocoles, relatives à l'identité des parties, au prix des prestations, aux caractéristiques de la fourniture, à la durée et aux conditions d'évolution ou de reconduction des contrats et protocoles, aux pénalités et sanctions contractuelles, 2° les informations relatives aux quantités livrées issues des comptages, des mesures de pression en aval du poste de livraison, des mesures de débit, ou de toutes autres mesures physiques effectuées par l'opérateur gazier sur les ouvrages de raccordement ou les installations d'un utilisateur de ces ouvrages ou installations.

« Livrable » : désigne tout résultat qui doit être réalisé par le Titulaire ou ses sous-traitants, conformément aux dispositions du contrat et des documents contractuels. Il peut s'agir d'un document, d'une fonctionnalité ou d'un programme développé spécifiquement pour GRDF.

PRA / PCA : le Plan de Reprise d'activités (PRA) et le Plan de Continuité d'Activité (PCA) sont deux mesures qui doivent permettre à une entreprise de survivre à un sinistre et de basculer sur un système de relève capable de prendre en charge les différents besoins informatiques de l'entreprise.

Le PCA permet de poursuivre l'activité sans interruption de service tandis que le PRA doit permettre de reprendre l'activité après une interruption.

« **Solution** » : désigne la solution cible proposée par le Soumissionnaire qui intègre tous les éléments matériels, logiciels (outillage etc.) licences et services (intégration, télésurveillance, maintenance etc.) requis.

« **Soumissionnaire** » : désigne les candidats à la présente consultation dont la candidature a été sélectionnée au regard de leurs capacités financière, professionnelle et technique et qui sont invités à remettre une offre conformément au présent Règlement de consultation.

1.3 Acronymes

CDC	Cahier Des Charges
CDP	Chef de Projet
GRC	Gouvernance, risque et conformité
GRDF	Gaz Réseau Distribution France
KPI	Key Performance Indicator – Indicateurs de mesure de la performance
PAQ	Plan d'Assurance Qualité
PAQM	Plan d'Assurance Qualité Maintenance
PAQP	Plan d'Assurance Qualité Projet
PAS	Plan d'Assurance Sécurité
RSSI	Responsable Sécurité des Systèmes d'Informations
SI	Système d'Information

SMSI	Système de Management de la Sécurité de l'Information

2 Prestations attendues

2.1 Lot 1 - Mise en place d'un Système de Management de la Sécurité de l'Information (SMSI)

Objectifs de la prestation : GRDF est en cours d'implémentation d'un Système de Management de la Sécurité de l'Information (SMSI), selon la norme ISO/IEC 27001 et les normes associées (la certification n'est pas envisagée pour l'instant). A ce titre, un accompagnement pourrait être demandé dans la finalisation du déploiement, ainsi que dans la mise en place de dispositifs de surveillance et d'amélioration continue du SMSI.

Il est à noter que les activités 1.1 (Mise en place de la Gouvernance relative au SMSI) et 1.2 (Mise en place du socle documentaire du SMSI) ci-dessous sont déjà initiées et en cours de réalisation. Selon l'avancée des travaux, la prestation pourrait se concentrer uniquement sur les activités 1.3 et 1.4.

Ref.	Activités	Description
1.1	Mise en place de la Gouvernance relative au SMSI	Définition de la Gouvernance SMSI : cadre organisationnel et responsabilités des différentes parties prenantes. Refonte de la PSSI (Politique de Sécurité des Systèmes d'Information) pour l'adapter aux nouveaux besoins et objectifs de sécurité de GRDF. Mise en place des différents comités (par exemples des comités de pilotage et de suivi) assurant le bon fonctionnement du SMSI.
1.2	Mise en place du socle documentaire du SMSI	Identification des politiques et procédures de sécurité de l'information manquantes pour répondre aux objectifs de la norme ISO/IEC 27001, aux réglementations auxquelles GRDF est soumis ou encore aux normes auxquelles GRDF veut se conformer. Formalisation des politiques et des procédures, prise en compte des aspects organisationnels et techniques. Etablissement d'un plan de formation et de sensibilisation pour les collaborateurs (internes et/ou externes).
1.3	Surveillance du SMSI	Définition du dispositif de surveillance du SMSI. Mise en place du dispositif, composé des audits et des contrôles, vérifiant la conformité aux exigences du SMSI et de l'Annexe A (livrée aux candidats qui seront sélectionnés). Evaluation régulière des risques liés à la sécurité de l'information et mise à jour des mesures de contrôle en conséquence (cf. chapitre 3.4).

1.4	Amélioration continue du SMSI	Prise en compte des résultats des actions de surveillance permettant d'identifier les domaines d'amélioration. Mise en œuvre des actions correctives et préventives pour améliorer en continu le SMSI. Mise à jour annuelle des documents et actions de surveillance pour s'assurer qu'ils restent à jour et adaptés aux évolutions du Système d'Information.

2.2 Lot 1 - Certifications/conformités/évaluation de la maturité

Objectifs de la prestation : réalisation d'évaluations et d'analyse d'écart sur plusieurs périmètres GRDF, selon des critères d'évaluations et d'analyse d'écart variés (SMSI, normes Sécurité, Directive Européenne, etc.).

Proposer et déployer un processus de veille réglementaire, permettant à GRDF d'identifier les impacts potentiels des nouvelles réglementations Sécurité.

Ref.	Activités	Description
2.1	Evaluation	Planification et réalisation d'évaluation de la sécurité. Les évaluations sécurité sont principalement organisationnelles et peuvent être sur plusieurs périmètres : SMSI, nouvelles directives européenne, nouvelle norme internationale. Evaluation de la conformité de GRDF sur les périmètres demandés et identification des écarts, des risques et des points d'amélioration. Rédaction d'un rapport d'évaluation incluant une synthèse managériale et comprenant les constats, les recommandations et un plan d'action pour corriger les écarts et renforcer la conformité.
2.2	Analyse d'écart	Planification d'analyses d'écart sur le Système d'Information. Les analyses peuvent avoir plusieurs formes : analyse du SMSI, écart vis-à-vis de nouvelles directives européennes ou normes internationales. Pour information : La réalisation des audits se fera dans le cadre d'une autre prestation (hors périmètre de cette consultation) : Evaluation de la conformité de GRDF et identification des écarts, des risques et des points d'amélioration. Rédaction d'un rapport détaillé incluant une synthèse managériale présentable en l'état au comité directeur de la DSI ou au comité exécutif de GRDF et comprenant les constats, les recommandations et un plan d'action pour corriger les écarts et renforcer la conformité. Les attendus concernant les analyses d'écart sont plus importants que pour les évaluations en matière de méthodologie, de contrôles, d'observations, ainsi que de qualité du rapport (exhaustivité des non-conformités et des recommandations).

2.3	Analyse réglementaire cybersécurité	Analyse et interprétation des nouvelles réglementations cybersécurité pour déterminer leurs implications pour GRDF. Etude d'impact sur le référentiel documentaire.

2.3 Lot 1 - Pilotage

Objectifs de la prestation : accompagner GRDF dans le suivi des différents plans d'action cybersécurité et dans l'assistance à la chefferie des projets GRC de cybersécurité.

Ref.	Activités	Description
3.1	Suivi de plans d'action	Suivi régulier de l'avancement des différents plans d'action relatifs à la cybersécurité, en vérifiant l'achèvement des tâches et la réalisation des objectifs dans les délais impartis. Identification des problématiques rencontrées lors de la mise en œuvre des plans d'action et proposition des solutions. Proposition de réévaluation et d'ajustement des plans d'action, en fonction des évolutions des besoins de GRDF et de l'environnement.
3.2	Assistance chefferie de projet	Accompagnement du chef de projet dans la définition des objectifs, des priorités et des ressources nécessaires pour la mise en œuvre des actions liées à la sécurité. Conseil vis-à-vis du chef de projet sur les sujets relatifs à la cybersécurité.

2.4 Lot 2 - Gestion des risques au niveau stratégique

Objectifs de la prestation : établissement d'une stratégie de gestion des risques stratégiques GRDF. Réalisation d'analyses de risques stratégiques EBIOS RM, consolidation des risques de différentes sources, proposition et suivi d'indicateurs de performances du SMSI et de la gestion des risques.

Formalisation d'un programme d'audit (ISO 19011) et de la politique d'homologation Sécurité de GRDF.

Ref.	Activités	Description
4.1	Analyse de risque stratégique	Réalisation d'analyses de risque sur des processus d'entreprise ou sur l'ensemble de GRDF en utilisant la méthodologie EBIOS RM. Identification des vulnérabilités, des menaces et des impacts potentiels afin de prioriser les risques, proposition d'une option de traitement des risques adaptée. Rédaction d'un rapport d'analyse de risque détaillé, incluant une synthèse managériale.
4.2	Consolidation des risques	Réalisation de l'analyse et de la consolidation des informations sur les risques provenant de différents rapports d'audit et des analyses de risques.

		Synthèse des informations afin de fournir une vue globale et cohérente des risques, identification des tendances, des corrélations et des actions prioritaires atténuant les risques. Rédaction d'un rapport de consolidation des risques facilitant la prise de décision et le suivi des actions.
4.3	Programme d'audit	Etablissement d'un programme d'audits conforme à la norme ISO 19011, incluant la planification et le suivi des audits de sécurité de l'information. Identification des domaines clés à auditer et des ressources nécessaires pour mener à bien les audits, selon les objectifs de sécurité de GRDF. Mise en place d'un processus de suivi et d'amélioration continue des audits pour garantir leur pertinence et leur efficacité.
4.4	Politique d'homologation	Elaboration d'une politique d'homologation qui définit les processus d'homologation, les étapes, les exigences et les responsabilités. Formalisation de contrôles concernant la bonne implémentation des exigences définies dans la politique d'homologation. Formalisation d'un processus de suivi et de révision régulière de la politique d'homologation.
4.5	Tableau de bord indicateurs	Proposition d'indicateurs clés de performance (KPI) pertinents pour la gestion des risques et les différents aspects du SMSI. Formalisation d'une politique concernant la collecte, l'analyse et la présentation des indicateurs. Conception d'un tableau de bord d'indicateurs afin de surveiller et mesurer la performance des processus de gestion des risques et du SMSI.

2.5 Lot 3 - Gestion des risques au niveau opérationnel

Objectifs de la prestation : déploiement de la Politique d'Homologation formalisée précédemment (cf. chapitre 3.4). Réalisation d'analyses de risques sécurité dans le cadre des projets d'homologations.

Ref.	Activités	Description
5.1	Accompagnement à l'homologation	Mise en œuvre du processus d'homologation sur un ou plusieurs systèmes, en suivant la politique d'homologation de GRDF, en collaborant avec les équipes internes et externes tout au long du processus.
5.2	Analyse de risques Applications / Projets	Dans le cadre d'une homologation de sécurité, réalisation d'analyses de risque sur les applications ou les projets de GRDF en utilisant la méthodologie EBIOS RM (par défaut) ou autre. Identification des vulnérabilités, des menaces et des impacts potentiels afin de prioriser les risques, proposition d'une option de traitement des risques adaptée.

		Rédaction d'un rapport d'analyse de risque détaillé, incluant une synthèse managériale.
5.3	Réalisation de cartographies	Réalisation des cartographies des SIE, en vue de l'homologation.

3 Déroulement des prestations

3.1 Localisation

Les prestations se dérouleront principalement dans les locaux de GRDF en île de France, et notamment :

- Site de Condorcet : 6, rue Condorcet - 75009 Paris

Le Soumissionnaire sera amené à se déplacer et à intervenir sur des sites GRDF ou des sites partenaires de GRDF qui devraient être principalement localisés en Ile de France.

En fonction du contexte, certaines prestations peuvent être réalisées à distance.

3.2 Langue de travail

La langue de communication sera le français dans tous les travaux, que ceux-ci soient écrits ou oraux.

En revanche, les relations avec les différents éditeurs de solutions pourront être en anglais.

3.3 Moyens mis à disposition par GRDF

Le Titulaire disposera, si nécessaire, de postes de travail bureautique fourni par GRDF, avec les outils bureautiques classiques, ainsi que les outils techniques nécessaires aux prestations.

GRDF fournira également l'ensemble des documentations nécessaires au Titulaire pour réaliser les travaux. Les documents seront établis selon les modèles et normes de présentation en vigueur à GRDF.

Des badges d'accès seront fournis et devront être restitués impérativement en fin de prestation. Ceci est également valable pour tout matériel et documentation que le Titulaire recevra de GRDF durant sa mission.

3.4 Plages de présence

3.4.1 Horaires de référence

Le Titulaire assure les activités sur le site de GRDF, les jours ouvrés du lundi au vendredi.

Chaque intervenant du Titulaire se conforme aux horaires de travail en vigueur au sein de l'équipe à laquelle il est affecté sur une durée de huit heures. Chaque intervenant organise ses activités ordinaires de sorte de mener à bien les travaux prévus au présent cahier des charges à l'intérieur de la plage horaire de cette équipe.

3.4.2 Plages d'ouverture du site GRDF

A ce jour, les travaux peuvent être réalisés entre 7h00 et 21h00 sur le site de Condorcet. L'accès au site en dehors de ces horaires nécessite une dérogation pour raison de service.

3.4.3 Présence de nuit et hors jours ouvrés

A l'initiative de l'intervenant :

Pour travailler sur site GRDF de nuit (entre 21h00 et 7h00) et/ou hors jours ouvrés (samedi, dimanche, jours fériés), les intervenants doivent préalablement aviser la responsable de la prestation de GRDF et obtenir son accord formel.

Des autorisations des services de sécurité du site peuvent être nécessaires.

A l'initiative de GRDF :

Lorsqu'ils ont été effectués à la demande de GRDF, les travaux menés de nuit et hors jours ouvrés donnent lieu à des prestations complémentaires dans les conditions prévues au contrat qui sera établi entre le Titulaire et GRDF.

3.5 Compétences requises

Compétences communes aux 4 prestations	
Compétences techniques	Certification ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, ISO 27005 Risk Manager Implémentation de SMSI Analyses de Risques Sécurité (EBIOS RM) sur des organisations et des applications Homologation de Sécurité Framework de cybersécurité
Compétences générales	Capacité d'analyse et de synthèse Aisance dans la communication écrite et orale en Français Proactivité, force de proposition Faculté d'agir avec autonomie Capacité d'adaptation Sens du relationnel et de la négociation / Bonnes qualités d'écoute (au choix) Maîtrise de l'anglais technique Adaptabilité et curiosité technique Capacité de capitalisation

Expériences requises	
Mise en place d'un Système de Management de la Sécurité de l'Information	Au moins un profil de 5 ans d'expérience minimum, avec une expérience significative en implémentation d'un SMSI Profils de 3 ans d'expérience minimum en sus
Certifications/conformités/évaluation de la maturité	Profils de 3 ans d'expérience minimum
Pilotage : stratégie, suivi des actions sécurité, reporting	Profils d'1 an d'expérience minimum
Gestion des risques au niveau stratégique	Profils de 5 ans d'expérience minimum
Gestion des risques au niveau opérationnel	Au moins un profil de 5 ans d'expérience minimum, avec une expérience significative en homologation sécurité de systèmes d'information. Profils de 3 ans d'expérience minimum en sus