

**MARCHE DE «REALISATION DE PRESTATIONS D'AUDITS,
D'EXPERTISES ET D'ASSISTANCE POUR LE MAINTIEN ET LE
RENFORCEMENT DE LA SECURITE INFORMATIQUE DU SYSTEME
D'INFORMATION DE LA BIBLIOTHEQUE NATIONALE DE FRANCE»**

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

TABLE DES MATIERES

1. INTRODUCTION	3
1.1 OBJET DU DOCUMENT	3
1.2 OBJECTIF DU MARCHE	3
1.3 LES OBJECTIFS ET MISSIONS DE LA BNF.....	3
1.4 ORGANISATION ADMINISTRATIVE DE LA BIBLIOTHEQUE	4
1.5 LES DIFFERENTS SITES DE LA BNF	5
1.6 LE DEPARTEMENT DES SYSTEMES D'INFORMATION	5
1.6.1 Rôles et missions du DSI.....	5
1.6.2 Organisation du DSI.....	6
1.7 CONTEXTE TECHNIQUE	7
2. DESCRIPTION DES PRESTATIONS.....	7
2.1 NATURE DES PRESTATIONS	7
2.2 RAPPORTS D'AUDIT TECHNIQUE :	9
2.3 PROFIL DES INTERVENANTS	9
2.4 REUNION MANAGERIALE	9
3. PART FORFAITAIRE ET UNITES D'ŒUVRE :.....	10
3.1 PART FORFAITAIRE	10
3.2 PART A BONS DE COMMANDE (UNITES D'ŒUVRE).....	11
4. VERIFICATION DES PRESTATIONS.....	15

1. INTRODUCTION

1.1 OBJET DU DOCUMENT

Les prestations concernent le site François Mitterrand de la Bibliothèque nationale de France, quai François Mauriac à Paris.

L'ensemble des services est réalisé au profit de la personne publique domiciliée à l'adresse suivante :

Bibliothèque nationale de France
Quai François Mauriac
75706 Paris cedex 13

1.2 OBJECTIF DU MARCHE

La BnF offre de plus en plus de services destinés à un public externe via des applications Web, et par la même occasion ouvre son système d'information à des accès depuis l'extérieur. Il est nécessaire de pouvoir vérifier pour chacune de ces applications, leur niveau de sécurité, dès leur mise en service. Les fournitures d'expertises et de prestations d'assistance attendues de ce marché permettront :

- la réalisation d'audit des composants du SI chaque fois que nécessaire,
- de gérer en amont la sécurité dans les projets, en disposant en permanence d'un support pour la réalisation d'audit en cas de nouvelle application à mettre en production,
- de disposer d'expertises externes, pour aider la BnF à améliorer en cas de besoin sa politique de sécurité.

1.3 LES OBJECTIFS ET MISSIONS DE LA BNF

La Bibliothèque nationale de France a été créée par le décret 94.3 du 3 janvier 1994 aujourd'hui codifié aux articles R. 341-1 à R. 341-21 du code du patrimoine avec pour mission notamment de « *collecter, de cataloguer, de conserver et d'enrichir tous les champs de la connaissance, le patrimoine national dont elle a la garde, en particulier le patrimoine de langue française ou relatif à la civilisation française* ». Elle a repris à sa création les fonds, missions, droits et obligations notamment de la Bibliothèque Nationale.

La Bibliothèque nationale de France répond à deux principaux objectifs :

- ◆ en tant que bibliothèque patrimoniale, chargée de recueillir, conserver et enrichir le patrimoine documentaire national,
 - suivre une politique patrimoniale et documentaire allant au-delà du Dépôt Légal, notamment, par une démarche cohérente d'acquisition d'ouvrages français et étrangers ;
 - utiliser, au regard de l'importance des collections et de l'état de certaines d'entre elles, les moyens de gestion, de conservation et de restauration, proposés par les technologies les plus modernes ;
- ◆ en tant que bibliothèque de recherche encyclopédique,
 - satisfaire des publics différenciés : chercheurs, mais aussi « grand public », au cours de leurs activités culturelles ou professionnelles, dans le cadre d'une recherche suivie ou occasionnelle ;
 - traiter des disciplines variées et en plein essor : les sciences humaines, les sciences politiques, juridiques et économiques, les sciences exactes et les disciplines technologiques ;
 - prendre en compte le champ de la production éditoriale étrangère ;
 - couvrir des champs documentaires complétant le champ de l'écrit, par l'accès aux fonds audiovisuels et supports numériques notamment et plus généralement l'accès aux formes nouvelles d'édition ;
 - s'ouvrir à la communication vers l'extérieur, au sein d'un réseau fédérant les principales bibliothèques françaises, municipales et universitaires, et étrangères.

La mission patrimoniale

La Bibliothèque nationale de France assure, notamment sur les sites François – Mitterrand et Bussy Saint-Georges, la collecte, le signalement, la conservation et la communication du patrimoine d'imprimés, de périodiques, de

documents audiovisuels et multimédias. Les missions patrimoniales relatives aux collections spécialisées sont assurées sur le site de Richelieu.

Elle assure également le catalogage scientifique de ces documents, et produit la bibliographie nationale, y compris en favorisant d'importants programmes de catalogage rétrospectifs.

La mission documentaire et la politique de réseaux

La Bibliothèque nationale de France complète la collecte de la production nationale par une politique systématique d'acquisitions étrangères, et mène pour compléter ses propres ressources, une politique de partenariat et de réseau avec d'autres institutions ou centres documentaires français ou étrangers.

Cette mission documentaire répond en particulier aux données suivantes :

- ◆ création d'un département « sciences et techniques », développement du fonds d'histoire des sciences,
- ◆ fonds de recherches et documentation professionnelle en droit, économie, sciences politiques,
- ◆ approfondissement de la spécialisation de l'ancienne Bibliothèque Nationale en histoire et littérature,
- ◆ augmentation importante du nombre d'usuels en libre accès.

La politique de réseau documentaire obéit en priorité à l'objectif de coopération avec d'autres institutions comme :

- ◆ les organismes chargés du Dépôt Légal, pour les actions de surveillance partagée du Dépôt Légal (contrôle croisé) et de pré-catalogage,
- ◆ les bibliothèques associées, pour le développement concerté des collections, l'échange de documents et de services
- ◆ les bibliothèques nationales et les grandes bibliothèques de recherche étrangères.

La Bibliothèque nationale de France pilote la Mission du Catalogue Collectif de France. A ce titre, elle favorise des opérations de conversion rétrospective informatique des catalogues de certaines bibliothèques, afin de disposer d'un seuil minimum de notices informatisées.

La mission d'exploitation scientifique des fonds

L'ensemble des activités précédemment décrites (collecte, signalement, conservation, communication, enrichissement documentaire) créent les conditions d'une exploitation scientifique, notamment par les chercheurs, de collections d'importance inégale.

La mission culturelle

La Bibliothèque nationale de France fait connaître et valorise ses collections et ses missions à travers une politique culturelle qui se traduit par : des publications, colloques, conférences, expositions, actions pédagogiques et de formation.

Pour une présentation détaillée de l'histoire et des activités de la BnF, voir le site <http://www.bnf.fr>.

1.4 ORGANISATION ADMINISTRATIVE DE LA BIBLIOTHEQUE

Sous la Présidence de Monsieur Gilles Pecout et la Direction générale de Monsieur Philippe LONNE, la Bibliothèque nationale de France est organisée en cinq Directions, quatre Délégations:

- ◆ la Direction des Collections (DCO) a en charge la gestion des collections ; elle est organisée en 14 départements :
- ◆ la Direction des Services et des Réseaux (DSR), organisée en 6 départements;
- ◆ la Direction de l'Administration et du Personnel (DAP) ; organisée en 3 départements et une direction déléguée:
- ◆ la Direction des publics (DPU) organisée en 2 départements
- ◆ la Direction du développement culturel et du musée (DDC), organisée en 2 départements

Dépendant de la Direction Générale :

- ◆ la Délégation à la stratégie (DSG)

- ◆ la Délégation aux relations internationales (DRI)
- ◆ la Délégation au mécénat (DME)
- ◆ la Délégation à la communication (COM)

L'organigramme de la BnF est disponible à l'adresse suivante: <https://multimedia-ext.bnf.fr/pdf/organigramme.pdf>

1.5 LES DIFFERENTS SITES DE LA BNF

Le site principal de la BnF où sont situés l'essentiel des serveurs et près de 90% des postes de travail, périphériques et équipements réseaux du SI, est le site :

Site François Mitterrand

quai François Mauriac - 75706 Paris Cedex 13

Sur ce site, coexistent deux espaces recevant du public:

- la bibliothèque d'étude du Haut-de-Jardin dont les collections issues d'acquisition sont en libre accès
- la bibliothèque de recherche du Rez-de-Jardin où sont accessibles les collections patrimoniales de la BnF

Les autres sites sont :

Centre technique de Bussy-Saint-Georges

14, avenue Gutenberg - 77607 Bussy-Saint-Georges Cedex 03

Site Richelieu

58, rue de Richelieu et 2, rue Louvois – 75084 Paris Cedex 02

Bibliothèque de l'Arsenal

1, rue de Sully – 75004 Paris

Bibliothèque-Musée de l'Opéra

Place de l'Opéra – 75009 Paris

Centre Joël Le Theule

Le Château - 72300 Sablé-sur-Sarthe

Maison Jean-Vilar

8, rue de Mons – 84000 Avignon

1.6 LE DEPARTEMENT DES SYSTEMES D'INFORMATION

Le Département des Systèmes d'Information fait partie de la Direction des Services et des Réseaux.

1.6.1 ROLES ET MISSIONS DU DSI

La BnF a confié au Département des Systèmes d'Information les missions d'exploitation, de maintien en condition opérationnelle et la maîtrise d'ouvrage du développement des systèmes d'information.

Le DSI doit donc assumer :

- L'exploitation et le maintien en condition opérationnelle de l'infrastructure du SI (serveurs, réseaux, postes de travail) ;
- L'exploitation et le maintien en condition opérationnelle des versions applicatives du SI actuellement en service ;
- La maîtrise d'œuvre ou la maîtrise d'ouvrage déléguée du développement des nouvelles applications demandées par les utilisateurs et priorisée par la Direction Générale.

Le DSI joue donc le rôle d'**opérateur** de la version courante exploitée, tout en restant une **maîtrise d'ouvrage de « produit »** (dans le cas de nouvelles applications, par exemple). La responsabilité d'opérateur lui confère les obligations d'un prestataire de services dont l'engagement est d'assurer un ensemble de prestations identifiées pour un niveau de qualité de service défini.

Afin de garantir les engagements de qualité de service et de poursuivre les missions de développement des versions du SI et les missions de prospective inhérentes à un gestionnaire des systèmes d'information, il a été décidé de confier les tâches répétitives et "industrialisables" à un fournisseur spécialisé.

Dans la conduite de la production et du maintien en condition opérationnelle, le DSI est un **opérateur** dont la vocation se résume au maintien des objectifs initiaux de services et de performances de la version courante exploitée.

Dans le cas du maintien en condition opérationnelle des applications du système d'information, le DSI est une **maîtrise d'œuvre de produit** qui assure, avec ses forces internes ou en sous-traitant une partie de ces travaux, les travaux de maintenance corrective, curative et évolutive.

Dans le cas de la conduite des évolutions, le DSI est une **maîtrise d'ouvrage de produit**, guidée par le contexte méthodologique de l'ingénierie de grands systèmes : pilotage de projets, conception de systèmes, développement, recettes.

1.6.2 ORGANISATION DU DSI

Le Département des Systèmes d'Information (DSI) de la BnF est composé actuellement de 125 personnes. Il couvre tous les métiers du cycle de vie d'un système informatique : définition des besoins, conception, développement, intégration, recette, exploitation, accompagnement et support.

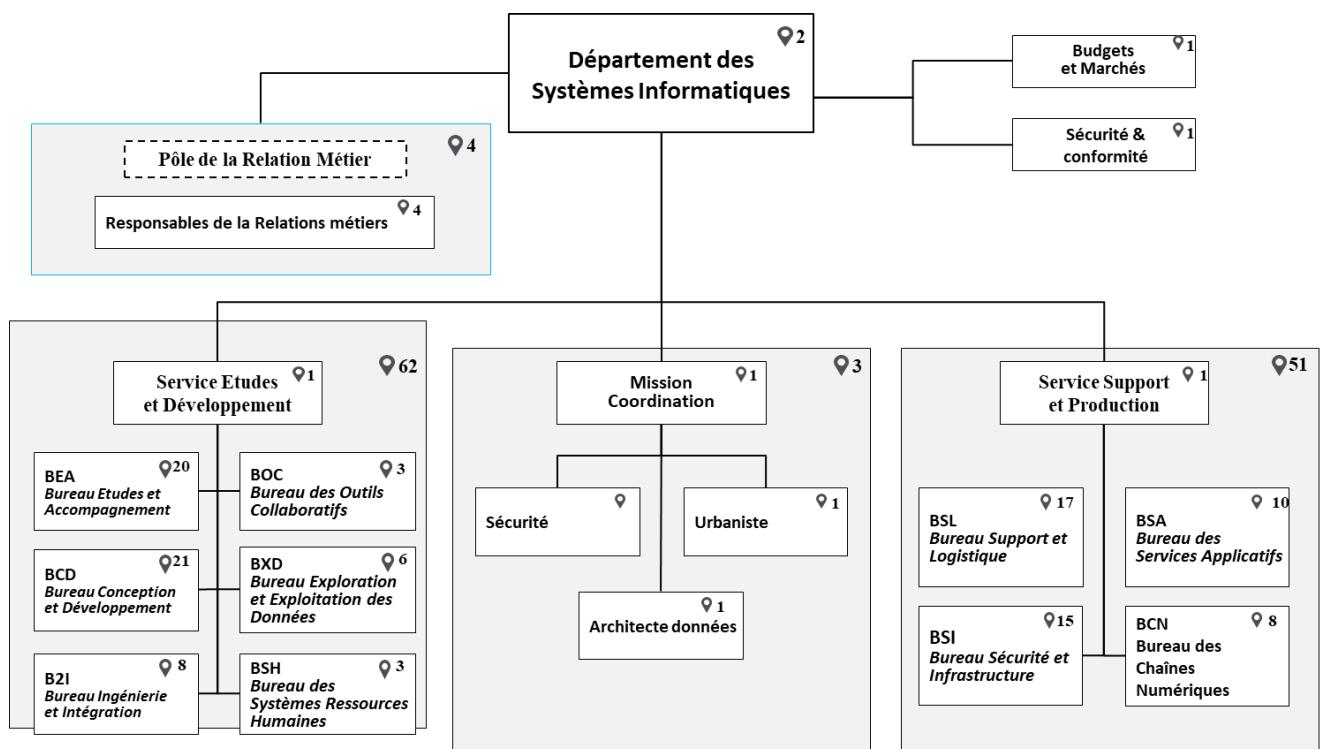


Figure 1 : Organigramme DSI

Le DSI est décomposé en deux services principaux (le service support et production et le service études et développement) et une mission de coordination de projets.

La mission coordination et projets assure le suivi et la coordination des projets transverses et importants du DSI.

1.7 CONTEXTE TECHNIQUE

Le système d'information géré par le DSI est composé de systèmes et d'applicatifs d'une très grande diversité que l'on peut décomposer de la manière suivante :

- Une architecture client/serveur à trois niveaux, avec plus de 220 applications réparties dans 7 groupes fonctionnels (CCF, EXP, PFF, PRO, PUB, SEC, WEB), et représentant 21 chaînes applicatives,
- Un système de billetterie et de contrôles d'accès,
- Un système de gestion des temps et des activités,
- Un système de gestion des Ressources Humaines assuré par un progiciel (HR-ACCESS),
- Un système de gestion des Ressources Financières assuré par un progiciel (SIREPA puis PEP PREMIUM à compter de janvier 2026),
- Un système de gestion du Bulletinage (Millénium),
- Un système de gestion des activités du service reproduction (NADAR),
- Un système de catalogage pour les collections spécialisées (CatXML),
- Un système de pilotage (SIPIL),
- Un système de préservation et d'archivage réparti (SPAR).

Une chaîne applicative est constituée d'applications et de serveurs offrant un ensemble fonctionnel cohérent de services. Les chaînes applicatives assemblées au sein d'un même groupe fonctionnel présentent des criticités et des contraintes de fonctionnement similaires.

Infrastructures techniques:

Serveurs (physique ou logique) : Unix (Aix, Linux) et X86 (Windows/VMWare/ Proxmox)

Postes de travail : Windows

Environnement de développement

Les développements applicatifs sont réalisés principalement en langage C++ et Java J2E.

2. DESCRIPTION DES PRESTATIONS

Les prestations de ce marché se décomposent en une part forfaitaire (PF), comportant deux postes, et une part à commandes sur la base de prix unitaires reposant sur des unités d'œuvre (UO). La décomposition retenue permet une répartition des prestations de manière transverse aux métiers et aux besoins de la DSI.

2.1 NATURE DES PRESTATIONS

Toutes les prestations nécessitant une présentation sur place sur le site François – Mitterrand peuvent, en cas d'impossibilité majeure, être remplacées par une présentation à distance en visio conférence. Dans ce cas, si le titulaire ne dispose pas d'une solution technique pour ce faire compatible avec l'environnement du SI de la BnF, la BnF mettra à disposition sa propre solution.

- **Audit technique boîte «noire»** : Cet audit technique a pour but d'identifier par des tests de vulnérabilités et d'intrusion la sécurité d'un système (cible) depuis des zones publiques (interne ou externe de la BnF). Le titulaire ne dispose d'aucune information préalable sur la cible auditée. Le ou les cibles de l'audit peuvent être indifféremment des composants matériels ou logiciels de l'infrastructure du SI et des applications.

Cette prestation inclut :

- L'audit technique,
- La fourniture d'un rapport technique détaillé (voir chapitre rapport technique) incluant une synthèse managériale (résumé du rapport détaillé à destination de l'encadrement),
- Une présentation des résultats à la BnF sur le site François - Mitterrand.

- **Audit technique boîte «grise»** : Cet audit technique a pour but d'identifier par des tests de vulnérabilité et d'intrusion la sécurité d'un système (cible). Le titulaire dispose de droits «utilisateur» du système audité. Le ou les cibles de l'audit peuvent être indifféremment des composants matériels ou logiciels de l'infrastructure du SI et des applications.

Cette prestation inclut :

- L'audit technique correspondant au nombre d'unités d'oeuvre,
- La fourniture d'un rapport technique (voir chapitre rapport technique) incluant une synthèse managériale,
- Une présentation des résultats à la BnF sur le site François - Mitterrand.

- **Audit technique boîte «blanche»** : Cet audit technique doit permettre d'analyser la sécurité d'un système en ayant des droits avancés et de disposer de toutes informations disponibles sur l'infrastructure auditée. Le ou les cibles de l'audit peuvent être indifféremment des composants matériels ou logiciels de l'infrastructure du SI ou des applications.

Cette prestation inclut :

- L'audit technique,
- La fourniture d'un rapport technique (voir chapitre rapport technique) incluant une synthèse managériale,
- Une présentation des résultats à la BnF sur le site François - Mitterrand.

- **Assistance technique opérationnelle** : Le titulaire doit disposer de personnels expérimentés dans les différents domaines techniques composant un système d'information (système, middleware, base de données, messagerie, sécurité, réseau, etc..). L'intervenant devra proposer, sous forme de procédures détaillées et opérationnelles, les solutions techniques de correction ou d'amélioration liées à un environnement technique ayant fait l'objet de recommandations dans le cadre de ce marché au travers des trois prestations d'audit possibles. En fonction des besoins de la BnF, l'intervenant doit assister la BnF pour la mise en œuvre des solutions techniques qu'il préconise à la suite de ses audits sur l'infrastructure du système d'information de la BnF.

Toute solution technique devra prendre en compte les caractéristiques techniques, fonctionnelles et opérationnelles du SI.

Cette prestation inclut :

- La fourniture de documents intégrant les solutions techniques et les procédures opérationnelles de mise en œuvre,
- L'accompagnement opérationnel de la BnF sur site.

- **Audit technique de revue de code sécurité** : Cet audit technique doit permettre d'identifier des failles de sécurité de code. Les langages de développement utilisés sont majoritairement le langage C++ et le Java J2E.

L'expression de l'unité d'œuvre de ce type de prestation est un «nombre de lignes analysées».

Cette prestation inclut :

- L'audit technique de code,
- La fourniture d'un rapport technique (voir chapitre rapport technique) incluant une synthèse,
- Une présentation des résultats à la BnF sur le site de François - Mitterrand.

- **Transfert de compétence « sécurité dans le développement logiciel »** : Le titulaire en collaboration avec la BnF doit proposer des prestations de transfert de compétences sur le développement de codes sécurisés suite à un audit technique de revue de code sécurité par exemple. Le profil des personnels BnF du département du système d'information concerné par ce transfert seront essentiellement des chefs de projet et/ou des ingénieurs confirmés dans la conception et le développement de logiciels. La séance au cours de laquelle ce transfert de compétence se déroulera ne dépassera pas 1 journée et 10 personnes maximum.

L'expression de l'unité d'œuvre de ce type de prestation est la «séance de transfert de compétence».

Cette prestation inclut :

- Un support de présentation,
- Le transfert de compétence à la BnF sur le site François – Mitterrand, ou en cas d'impossibilité majeure à distance, par visio conférence.

La BnF mettra à la disposition du titulaire une salle de formation sur le site François - Mitterrand (vidéo projecteur, tableaux, poste informatique peuvent être fournis à la demande) ou le cas échéant la solution de visio conférence si le titulaire ne dispose pas de sa propre solution ou d'une solution compatible avec l'environnement du SI de la BnF.

Expertise dans le domaine de la sécurité informatique : Prestations d'expertise technique d'investigation et d'analyse d'événement de sécurité du système d'information ou d'expertise en politique de sécurité. L'unité principale d'expression de ce prix unitaire est la journée d'expertise.

Cette prestation inclut :

- Une prestation d'expertise,
- La fourniture de documents issus de l'expertise.

Suivi régulier du niveau de sécurité des applications webs : Cette prestation doit permettre de suivre de manière régulière, sur une année, le niveau de sécurité des applications webs publiques de la BnF. Cette prestation consiste en la réalisation de 6 audits techniques de type « boîte blanche » ou « boîte grise » ou « boîte noire » en fonction des besoins de la BnF.

Cette prestation inclut :

- Une prestation d'expertise comportant les 6 audits décrits ci-dessus, réalisés de manière successive (un audit boîte noire suit un audit boîte blanche qui suit lui-même un audit boîte grise, sachant que l'ordre doit être aléatoire),
- La fourniture d'un rapport technique détaillé issu de chaque expertise,
- Une présentation des résultats de chaque expertise à la BnF sur le site François - Mitterrand.

Audit de type CTI (Cyber Threat Intelligence) : Cette prestation doit permettre de suivre en tant que de besoin l'exposition connue de la BnF par d'autres sur le web voire le « dark » web une année. Les recherches doivent permettre d'agréger, de corréler et d'analyser des informations provenant de différentes sources.

Cette prestation inclut :

- Une prestation d'expertise et de recherche des menaces externes,
- La fourniture d'un rapport technique détaillé incluant les recommandations.

2.2 RAPPORTS D'AUDIT TECHNIQUE :

Suivant la nature des prestations, les rapports seront organisés par domaine technique BnF ou/et par unité organisationnelle de la BnF. Ils seront rédigés de manière à rendre autonomes chaque partie du rapport (sans lien les unes avec les autres). Cette décomposition doit permettre une diffusion plus appropriée à l'organisation de l'établissement.

Chaque rapport intégrera un tableau de synthèse incluant pour chaque risque de sécurité : les recommandations associées ainsi que son niveau de criticité.

Les rapports intégreront pour chaque vulnérabilité le scénario d'exploitation de la faille de sécurité, ainsi que les degrés de difficultés dans la mise en œuvre des corrections qui peuvent être simple (pas de niveau d'expertise indispensable couplé à une durée de réalisation courte), raisonnable (niveau d'expertise normal couplé à une durée de réalisation moyenne) ou complexe (niveau d'expertise élevé couplé à une durée de réalisation importante).

Les rapports contiendront également une synthèse managériale.

Chaque commande devra faire l'objet d'un rapport distinct.

2.3 PROFIL DES INTERVENANTS

Le titulaire veillera pour l'exécution du marché à missionner des collaborateurs ayant les compétences et l'expérience professionnelle suffisantes pour atteindre dans le temps imparti les objectifs qualitatifs et quantitatifs associés à chaque prestation.

2.4 REUNION MANAGERIALE

Le titulaire présentera chaque année à la BnF, au cours d'une réunion de type managérial, une synthèse de son activité et les résultats obtenus au cours de l'année. Le titulaire présentera un bilan de la sécurité des systèmes expertisés (ses points positifs/négatifs) et si nécessaire des risques associés.

3. PART FORFAITAIRE ET UNITES D'ŒUVRE :

La part forfaitaire et la part à bons de commandes telles qu'elles résultent de l'offre du titulaire, figurent dans l'acte d'engagement et ses annexes.

Pour les prix unitaires de la part à commandes, ceux-ci s'entendent tous frais incluant les coûts d'encadrement et de structure.

3.1 PART FORFAITAIRE

La part forfaitaire comporte deux postes définis ci-après :

Poste 1 (de la part forfaitaire) : Audit du domaine Bnf.fr
<p>Objet : Audit technique basé sur des tests de vulnérabilité et d'intrusion de type «Boîte noire» du domaine Bnf.fr.</p> <p>Cette prestation d'audit de type boîte noire, doit se dérouler, une fois par an, en tenant compte des phases suivantes :</p> <ol style="list-style-type: none"> 1. Phase préparatoire : Cartographie du SI L'objectif de cette phase est de recenser depuis Internet, les différentes adresses IP et sites Web de la BnF. Cette cartographie permettra de déterminer les points d'entrée potentiels via Internet aux différents SI de la BnF susceptibles d'être exploités pour la connaissance de données sensibles ou d'éléments de description sur ses infrastructures. 2. Phase 1 - Recueil d'informations L'objectif de cette phase est de recueillir l'ensemble des informations nécessaires pour réaliser le test d'intrusion. 3. Phase 2 - Recherche de vulnérabilités Le titulaire détermine si les équipements identifiés présentent des vulnérabilités connues et susceptibles de compromettre l'infrastructure auditée. 4. Phase 3 - Exploitation des vulnérabilités Avec l'accord de la BnF, le titulaire exploitera les outils mis au point lors de la phase 2 et tentera de se connecter aux serveurs identifiés, afin d'obtenir un accès non autorisé à ces derniers. <p>À noter qu'aucun test de type déni de service n'est effectué sur les serveurs ou applications, afin d'assurer une continuité de service tout au long de l'audit.</p> <p>Le début d'exécution et le calendrier d'exécution des prestations incluses dans ce poste sont fixés d'un commun accord avec le titulaire. Le calendrier ainsi retenu sera notifié par la BnF par ordre de service au titulaire (cf article 1.4 du CCAP).</p> <p>Prestations : Réalisation de l'audit technique depuis un réseau public interne ou externe (Internet). La prestation inclut la fourniture d'un rapport technique détaillé de l'audit technique et la tenue d'une réunion de présentation du rapport à la BnF.</p> <p>Réalisation type: Audit à l'aveugle depuis une source externe.</p> <p>Fréquence de réalisation : Dans le cadre du forfait, le poste 1 sera réalisé par le titulaire une fois par an</p>

Poste 2 (de la part forfaitaire) : Audit de suivi régulier
<p>Objet : Suivi régulier du niveau de sécurité des applications webs – Audit technique basé sur des tests de vulnérabilité et d'intrusion d'applications webs.</p> <p>Le début d'exécution et le calendrier d'exécution des prestations incluses dans ce poste sont fixés d'un commun accord avec le titulaire. Le calendrier ainsi retenu sera notifié par la BnF par ordre de service au titulaire (cf article 1.4 du CCAP).</p> <p>Unité : Un audit technique, d'une durée d'une journée, tous les deux mois (soit au total 6 audits techniques par an)</p> <p>Prestations : Réalisation de 6 audits techniques de type « boîte blanche » ou « boîte grise » ou « boîte noire » en fonction des besoins de la BnF. La prestation inclut la fourniture de 6 rapports techniques détaillés de l'audit technique et de 6 réunions de présentation des résultats du rapport à la BnF.</p> <p>Réalisation type: Audit de 3 URL de sites webs publics choisies chaque mois par la BnF.</p> <p>Fréquence de réalisation : Dans le cadre du forfait, le poste 2 sera réalisé par le titulaire six fois par an, soit un audit tous les deux mois.</p>

3.2 PART A BONS DE COMMANDE (UNITES D'ŒUVRE)

Les bons de commande peuvent être passés sur la base des prix unités d'œuvre suivants :

Prix 1 basé sur l'unité d'œuvre 1 (UO1) : Audit à la demande du domaine Bnf.fr
<p>Objet : Audit technique basé sur des tests de vulnérabilité et d'intrusion de type «Boîte noire» du domaine Bnf.fr.</p> <p>Cette prestation sera commandée tant qu'il y en aura besoin dans l'année, une fois celui de la part forfaitaire réalisée. Cette prestation d'audit de type boîte noire, doit se dérouler en tenant compte des phases suivantes :</p> <ol style="list-style-type: none"> 1. Phase préparatoire : Cartographie du SI L'objectif de cette phase est de recenser depuis Internet, les différentes adresses IP et sites Web de la BnF. Cette cartographie permettra de déterminer les points d'entrée potentiels via Internet aux différents SI de BNF susceptibles d'être exploités pour la connaissance de données sensibles ou d'éléments de description sur ses infrastructures. 2. Phase 1 - Recueil d'information L'objectif de cette phase est de recueillir l'ensemble des informations nécessaires pour réaliser le test d'intrusion. 3. Phase 2 - Recherche de vulnérabilités Le titulaire détermine si les équipements identifiés présentent des vulnérabilités connues et susceptibles de compromettre l'infrastructure auditée. 4. Phase 3 - Exploitation des vulnérabilités Avec l'accord de la BnF, le titulaire exploitera les outils mis au point lors de la phase 2 et tentera de se connecter aux serveurs identifiés, afin d'obtenir un accès non autorisé à ces derniers. <p>À noter qu'aucun test de type déni de service n'est effectué sur les serveurs ou applications, afin d'assurer une continuité de service tout au long de l'audit. Le début d'exécution et le calendrier d'exécution des prestations incluses dans cette UO1 sont fixés d'un commun accord avec le titulaire lors de la commande. Le calendrier ainsi retenu sera notifié par la BnF dans le bon de commande.</p> <p>Prestations : Réalisation de l'audit technique depuis un réseau public interne ou externe (Internet). La prestation inclut la fourniture d'un rapport technique détaillé de l'audit technique et la tenue d'une réunion de présentation du rapport à la BnF.</p> <p>Réalisation type: Audit à l'aveugle depuis une source externe.</p>

Prix 2 basé sur l'unité d'œuvre 2 (UO2) : Contre audit du domaine Bnf.fr
<p>Objet : Audit technique basé sur des tests de vulnérabilité et d'intrusion de type «Boîte noire» du domaine Bnf.fr. Cette prestation d'audit peut être commandée à la suite d'un audit « Boîte noire » du domaine Bnf.fr, du Poste 1 de la part forfaitaire ou de l'UO1. Cette prestation d'audit de type boîte noire, doit se dérouler en réutilisant les informations trouvées lors de l'exécution de l'audit initial du domaine bnf.fr:</p> <ol style="list-style-type: none"> 1. Phase préparatoire : Cartographie du SI 2. Phase 1 - Recueil d'information 3. Phase 2 - Recherche de vulnérabilités 4. Phase 3 - Exploitation des vulnérabilités <p>À noter qu'aucun test de type déni de service n'est effectué sur les serveurs ou applications, afin d'assurer une continuité de service tout au long de l'audit. Le début d'exécution et le calendrier d'exécution des prestations incluses dans cette UO1 sont fixés d'un commun accord avec le titulaire lors de la commande. Le calendrier ainsi retenu sera notifié par la BnF dans le bon de commande.</p> <p>Prestations : Réalisation de l'audit technique depuis un réseau public interne ou externe (Internet). La prestation inclut la fourniture d'un rapport technique détaillé de l'audit technique et la mise en place d'une réunion de présentation du rapport à la BnF.</p> <p>Réalisation type: Audit à l'aveugle depuis une source externe.</p>

Prix 3 basé sur l'unité d'œuvre 3 (UO3) : Audit « Boîte noire » pour une URL**Objet** : Audit technique basé sur des tests de vulnérabilité et d'intrusion de type «Boîte noire».**Prestations** : Réalisation de l'audit technique depuis un réseau public interne ou externe (Internet). La prestation inclut la fourniture d'un rapport technique détaillé de l'audit technique et la mise en place d'une réunion de présentation du rapport à la BnF.**Réalisation type**: Audit d'un poste public situé dans une salle de lecture de la BnF.**Prix 4 basé sur l'unité d'œuvre 4 (UO4) : Audit « Boîte grise » pour une URL****Objet** : Audit technique basé sur des tests de vulnérabilité et d'intrusion de type «Boîte grise».**Prestations** : Réalisation de l'audit technique de type «boîte grise ». L'audit portera sur une application Web constituée d'une trentaine d'IHM, une vingtaine de champs de saisis et une trentaine de menus. La prestation inclut la fourniture d'un rapport technique détaillé de l'audit technique et la mise en place d'une réunion de présentation des résultats du rapport à la BnF.**Réalisation type**: Réalisation de l'audit d'une application Web de type 3 tiers.**Prix 5 basé sur l'unité d'œuvre 5 (UO5) : Audit « Boîte blanche » pour une URL****Objet** : Audit technique basé sur des tests de vulnérabilité et d'intrusion de type «Boîte blanche».**Prestations** : Réalisation de l'audit technique de type «boîte blanche». La boîte blanche fera généralement suite à un audit boîte grise de l'application. La prestation inclut la fourniture d'un rapport technique détaillé de l'audit technique et la mise en place d'une réunion de présentation du rapport à la BnF.**Réalisation type** : Revue de configuration d'une chaîne applicative.**Prix 6a basé sur l'unité d'œuvre 6 : (UO6a) : Mise en œuvre de corrections - Complexe****Objet** : Assistance technique opérationnelle pour la mise en œuvre de recommandations en matière de sécurité informatique.**Prestations** :

Cette prestation peut être commandée pour aider la personne publique à mettre en œuvre les recommandations/corrections qualifiées de type complexe (voir description dans le chapitre Rapport d'audit) dans les conclusions d'un précédent audit.

- la validation de recommandations dans les environnements du SI,
- une assistance technique opérationnelle auprès du personnel BnF pour la mise en œuvre des recommandations.

La prestation inclut la fourniture d'une documentation détaillée de solutions techniques et de procédures opérationnelles pour chaque recommandation.

Exemple de réalisation : Application des recommandations/corrections complexes suite à un audit technique constatant une vulnérabilité.**Prix 6b basé sur l'unité d'œuvre 6 : (UO6b) : Mise en œuvre de corrections - Raisonnable****Objet** : Assistance technique opérationnelle pour la mise en œuvre de recommandations en matière de sécurité informatique.**Prestations** :

Cette prestation peut être commandée pour aider la personne publique à mettre en œuvre les recommandations/corrections qualifiées de type raisonnable (voir description dans le chapitre Rapport d'audit) dans les conclusions d'un précédent audit.

- la validation de recommandations dans les environnements du SI,
- une assistance technique opérationnelle auprès du personnel BnF pour la mise en œuvre des recommandations.

La prestation inclut la fourniture d'une documentation détaillée de solutions techniques et de procédures opérationnelles pour chaque recommandation.

Exemple de réalisation : Application des recommandations/corrections raisonnables suite à un audit technique constatant une vulnérabilité

Prix 6c basé sur l'unité d'œuvre 6: (UO6c) : Mise en œuvre de corrections - Simple

Objet : Assistance technique opérationnelle pour la mise en œuvre de recommandations en matière de sécurité informatique.
Prestations : Cette prestation peut être commandée pour aider la personne publique à mettre en œuvre les recommandations/corrections qualifiées de type simple (voir description dans le chapitre Rapport d'audit) dans les conclusions d'un précédent audit. <ul style="list-style-type: none"> - la validation de recommandations dans les environnements du SI, - une assistance technique opérationnelle auprès du personnel BnF pour la mise en œuvre des recommandations. La prestation inclut la fourniture d'une documentation détaillée de solutions techniques et de procédures opérationnelles pour chaque recommandation.
Exemple de réalisation : Application des recommandations/corrections simples suite à un audit technique constatant une vulnérabilité

Prix 7 basé sur l'unité d'œuvre 7 (UO 7) : Revue de code de sécurité (5 000 lignes)
--

Objet : Sécurité du développement logiciel – audit technique de revue de code sécurité
Unité de base : 5000 lignes de code.
Prestations : Audit technique de revue de code sécurité. La prestation inclut un rapport de l'audit technique et la mise en place d'une réunion de présentation des résultats à la BnF.
Exemple de réalisation : Validation du code d'une application BnF.

Prix 8 basé sur l'unité d'œuvre 8 (UO 8) : Transfert de compétences sur une journée
--

Objet : Sécurité du développement logiciel – Transfert de compétences au personnel BnF sur une journée.
Prestations : Etablissement de l'objectif pédagogique/opérationnel. Transfert de compétences au personnel sur le site François - Mitterrand. L'objectif est la montée en compétence du personnel BnF dans le développement logiciel sécurisé. Avec l'accord de la BnF, la prestation peut se faire à distance. L'unité d'œuvre doit privilégier la prestation sur site.
Réalisation type : Session pour 10 personnes maximum «profil ingénieur de développement confirmé» sur le développement sécurisé d'une application Web avec les technologies différentes (Java, PHP, Python, ...).

Prix 9 basé sur l'unité d'œuvre 9 (UO 9) : Expertise d'urgence sur place

Objet : Expertise d'urgence – Expertise dans le domaine de la sécurité informatique.
Prestations : Prestations d'expertise sur place. L'unité d'œuvre sera mesurée en temps d'investigation par demi-journée d'un expert. Le personnel doit intervenir sur place ou à distance dans un délai de 4 heures à compter de la demande d'intervention de la BnF. La fourniture de documents issus de l'expertise est comprise dans cette unité (ce qui s'est passé, le processus d'investigation, les corrections apportées, les préconisations pour l'avenir).
Réalisation type : Investigation et analyse d'une infection virale sur des systèmes windows.

Prix 10 basé sur l'unité d'œuvre 10 (UO10) : Audit interne

Objet : Audit technique basé sur des tests de vulnérabilité et d'intrusion de type « boîte noire » et « boîte grise » sur le réseau interne de la BnF découpé en VLAN.

Pour la boîte grise, la BnF fournira les comptes utilisateurs nécessaires.

Cette prestation sera commandée tant qu'il y en aura besoin dans l'année, une fois celui de la part forfaitaire réalisée. Cette prestation d'audit de type boîte noire et boîte grise, doit se dérouler en tenant compte des phases suivantes :

1. Phase préparatoire : Cartographie du SI
L'objectif de cette phase est de recenser depuis Internet, les différentes adresses IP et sites Web de la BnF. Cette cartographie permettra de déterminer les points d'entrée potentiels via Internet aux différents SI de BnF susceptibles d'être exploités pour la connaissance de données sensibles ou d'éléments de description sur ses infrastructures.
2. Phase 1 - Recueil d'informations
L'objectif de cette phase est de recueillir l'ensemble des informations nécessaires pour réaliser le test d'intrusion.
3. Phase 2 - Recherche de vulnérabilités
Le titulaire détermine si les équipements identifiés présentent des vulnérabilités connues et susceptibles de compromettre l'infrastructure auditée.
4. Phase 3 - Exploitation des vulnérabilités
Avec l'accord de la BnF, le titulaire exploitera les outils mis au point lors de la phase 2 et tentera de se connecter aux serveurs identifiés, afin d'obtenir un accès non autorisé à ces derniers.

À noter qu'aucun test de type déni de service n'est effectué sur les serveurs ou applications, afin d'assurer une continuité de service tout au long de l'audit.

Prestations : Réalisation de l'audit technique depuis les réseaux logiques internes (agent, public filaire, public sans fil). La prestation inclut la fourniture d'un rapport technique détaillé de l'audit technique et la mise en place d'une réunion de présentation du rapport à la BnF.

Réalisation type: Audit à l'aveugle depuis une source externe.

Prix 11 basé sur l'unité d'œuvre 11 (UO11) : Contre audit interne

Objet : Audit technique basé sur des tests de vulnérabilité et d'intrusion de type «Boîte noire» du domaine Bnf.fr. Cette prestation d'audit peut être commandée à la suite d'un audit de type « boîte noire » et « boîte grise » sur le réseau interne de la BnF découpé en VLAN de l'UO10.

Pour la boîte grise, la BnF fournira comptes utilisateurs nécessaires.

Cette prestation d'audit de type boîte noire, doit se dérouler en réutilisant les informations trouvées lors de l'exécution de l'audit initial interne:

1. Phase préparatoire : Cartographie du SI
2. Phase 1 - Recueil d'information
3. Phase 2 - Recherche de vulnérabilités
4. Phase 3 - Exploitation des vulnérabilités

À noter qu'aucun test de type déni de service n'est effectué sur les serveurs ou applications, afin d'assurer une continuité de service tout au long de l'audit.

Le début d'exécution et le calendrier d'exécution des prestations incluses dans cette UO1 sont fixés d'un commun accord avec le titulaire lors de la commande. Le calendrier ainsi retenu sera notifié par la BnF dans le bon de commande.

Prestations : Réalisation de l'audit technique depuis un réseau public interne ou externe (Internet). La prestation inclut la fourniture d'un rapport technique détaillé de l'audit technique et la mise en place d'une réunion de présentation du rapport à la BnF.

Réalisation type: Audit à l'aveugle depuis une source externe.

Prix 12 basé sur l'unité d'œuvre 12 (UO 12) : Audit de type CTI (Cyber Threat Intelligence)
Objet : Audit préventif – Expertise dans le domaine de la sécurité informatique.
<p>Prestations : Prestations d'audit technique consistant à rechercher et détecter, en dehors du réseau de la BnF, les menaces susceptibles de l'impacter. L'objectif est d'aider la BnF à anticiper et se préparer à ces menaces.</p> <p>L'unité d'œuvre est définie comme une demi-journée d'investigation réalisée par un expert. Les prestations doivent intervenir dans un délai maximal de 4 heures à compter de la demande d'intervention de la BnF. La fourniture d'un rapport issu de l'investigation est comprise dans cette unité d'œuvre. Ce rapport devra inclure :</p> <ul style="list-style-type: none"> • Le contexte et le déroulé de l'intervention ; • Le détail du processus d'investigation ; • Les menaces ou vulnérabilités identifiées ; • Les mesures éventuelles à prendre ou à mettre en œuvre ; • Les préconisations à mettre en place pour renforcer la sécurité à l'avenir.
Réalisation type : Audit à l'aveugle depuis une source externe.

4. VERIFICATION DES PRESTATIONS.

Le titulaire se référera au chapitre «Vérification de l'exécution des prestations » du Cahier des Clauses Administratives Particulières (CCAP) de ce marché.