Compétences / Performances BLOC1			
BLOC1	**Support et mise à disposition de services informatiques**	**BLOC1**	**Support et mise à disposition de services informatiques**
B1.1	**Gérer le patrimoine informatique**	**B1.1**	**Gérer le patrimoine informatique**
B1.1.1	Recenser et identifier les ressources numériques	P1.1.1	Le recensement du patrimoine informatique est exhaustif et réalisé au moyen d'un outil de gestion des actifs informatiques.
B1.1.2	Exploiter des référentiels, normes et standards adoptés par le prestataire informatique	P1.1.2	Les référentiels, normes et standards sont mobilisés de façon pertinente.
B1.1.3	Mettre en place et vérifier les niveaux d'habilitation associés à un service	P1.1.3	Les droits mis en place correspondent aux habilitations des acteurs.
B1.1.4	Vérifier les conditions de la continuité d'un service informatique	P1.1.4	Les conditions de continuité et de reprise d'un service sont vérifiées et les manquements sont signalés.
B1.1.5	Gérer des sauvegardes	P1.1.5	Les sauvegardes sont réalisées dans les conditions prévues conformément au plan de sauvegarde.
		P1.1.6	Les restaurations sont testées et opérationnelles.
B1.1.6	Vérifier le respect des règles d'utilisation des ressources numériques	P1.1.7	Les écarts par rapport aux règles d'utilisation des ressources numériques sont détectés et signalés.
B1.2	**Répondre aux incidents et aux demandes d'assistance et d'évolution**	**B1.2**	**Répondre aux incidents et aux demandes d'assistance et d'évolution**
B1.2.1	Collecter, suivre et orienter des demandes	P1.2.1	En utilisant les outils adaptés, les demandes d'assistance ont été prises en compte, correctement diagnostiquées et leur traitement correspond aux attentes.
B1.2.2 B1.2.3	Traiter des demandes concernant les services réseau et système, applicatifs Traiter des demandes concernant les applications	P1.2.2	La réponse à une demande d'assistance est conforme à la procédure et adaptée à l'utilisateur.
		P1.2.3	La méthode de diagnostic de résolution d'un incident est adéquate et efficiente.
		P1.2.4	Une solution à l'incident est trouvée et mise en œuvre.
		P1.2.5	Le cycle de résolution des demandes respecte les normes et standards du prestataire informatique.
		P1.2.6	L'utilisation d'un logiciel de gestion de parc et d'incidents est maîtrisée.
		P1.2.7	Le compte rendu d'intervention est clair et explicite.
		P1.2.8	La communication écrite et orale est adaptée à l'interlocuteur.
B1.3	**Développer la présence en ligne de l'organisation**	**B1.3**	**Développer la présence en ligne de l'organisation**
B1.3.1	Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques	P1.3.1	L'image de l'organisation est conforme aux attentes et valorisée.
		P1.3.2	Les enjeux économiques liés à l'image de l'organisation sont identifiés et les obligations juridiques sont respectées.
		P1.3.3	Les mentions légales sont accessibles et conformes à la législation.
B1.3.2	Référencer les services en ligne de l'organisation et mesurer leur visibilité.	P1.3.4	La visibilité des services en ligne de l'organisation est satisfaisante.
B1.3.3	Participer à l'évolution d'un site Web exploitant les données de l'organisation.	P1.3.5	Le site Web a évolué conformément au besoin exprimé.
B1.4	**Travailler en mode projet**	**B1.4**	**Travailler en mode projet**
B1.4.1	Analyser les objectifs et les modalités d'organisation d'un projet	P1.4.1	Les objectifs et les modalités d'organisation du projet sont explicités.
		P1.4.2	L'analyse des besoins et de l'existant est pertinente.
B1.4.2	Planifier les activités	P1.4.3	Les activités personnelles sont planifiées selon une méthodologie donnée et les ressources humaines, matérielles et logicielles nécessaires sont mobilisées de manière efficace et pertinente.
		P1.4.4	Le découpage en tâches est réaliste.
		P1.4.5	Les livrables sont conformes.
		P1.4.6	Le projet est documenté.
B1.4.3	Évaluer les indicateurs de suivi d'un projet et analyser les écarts	P1.4.7	Un compte rendu clair et concis est réalisé et les écarts sont justifiés.
		P1.4.8	La communication écrite et orale est adaptée à l'interlocuteur.
B1.5	**Mettre à disposition des utilisateurs un service informatique**	**B1.5**	**Mettre à disposition des utilisateurs un service informatique**
B1.5.1	Réaliser les tests d'intégration et d'acceptation d'un service	P1.5.1	Des tests pertinents d'intégration et d'acceptation sont rédigés et effectués.
		P1.5.2	Les outils de test sont utilisés de manière appropriée.
		P1.5.3	Un rapport de test du service est produit.
B1.5.2 B1.5.3	Déployer un service Accompagner les utilisateurs dans la mise en place d'un service	P1.5.4	Un support d'information est disponible.
		P1.5.5	Les modalités d'accompagnement sont définies.
		P1.5.6	Le service déployé est opérationnel et donne satisfaction à l'utilisateur.
B1.6	**Organiser son développement professionnel**	**B1.6**	**Organiser son développement professionnel**
B1.6.1	Mettre en place son environnement d'apprentissage personnel	P1.6.1	Les besoins de formation sont identifiés pour assurer le support ou mettre à disposition un service.
		P1.6.2	L'environnement d'apprentissage personnel est délimité et expliqué.
B1.6.2	Mettre en œuvre des outils et stratégies de veille informationnelle	P1.6.3	**La veille est régulière et vise à :**
			P1.6.3.1 Repérer les techniques et technologies émergentes du secteur informatique ;
			P1.6.3.2 Utiliser de manière approfondie des moyens de recherche d'information ;
			P1.6.3.3 Renforcer de ses compétences.
B1.6.3	Gérer son identité professionnelle	P1.6.4	L'identité professionnelle est pertinente et visible sur un réseau social professionnel.
B1.6.4	Développer son projet professionnel		

Compétences / Performances BLOC2			
BLOC2	**Conception et développement d'applications**	**BLOC2**	**Conception et développement d'applications**
B2B.1	**Concevoir et développer une solution applicative**	**B2B.1**	**Concevoir et développer une solution applicative**
B2B.1.1	Analyser un besoin exprimé et son contexte juridique	P2B.1.1	La proposition de la solution applicative répond au besoin exprimé dans le cahier des charges y compris dans sa dimension contractuelle : P2B.1.1.1 La modélisation de l'application est conforme aux besoins ; P2B.1.1.2 La maquette des éléments applicatifs de la solution respecte les fonctionnalités exprimées ; P2B.1.1.3 Les spécifications de l'interface utilisateur répondent aux contraintes ergonomiques.
B2B.1.2	Participer à la conception de l'architecture d'une solution applicative		
B2B.1.3	Modéliser une solution applicative		
B2B.1.4	Exploiter les ressources du cadre applicatif (framework)		
B2B.1.5	Identifier, développer, utiliser ou adapter des composants logiciels	P2B.1.2	Le choix des composants logiciels à utiliser et/ou à développer est pertinent.
B2B.1.6	Exploiter les technologies Web pour mettre en œuvre les échanges entre applications, y compris de mobilité	P2B.1.3	Les composants logiciels sont validés par les procédures de tests unitaires et fonctionnels.
B2B.1.7	Utiliser des composants d'accès aux données	P2B.1.4	Un service Web est exploité pour échanger des données entre applications.
		P2B.1.5	Les données persistantes liées à la solution applicative sont exploitées à travers un langage de requête lié à la base de données qui peut être le langage de requête proposé par les échanges applicatifs des technologies Web, un langage de requête présent dans l'outil de correspondance objet-relationnel ou toute autre solution de persistance
B2B.1.8 B2B.1.9	Intégrer en continu les versions d'une solution applicative Réaliser les tests nécessaires à la validation ou à la mise en production d'éléments adaptés ou développés	P2B.1.6	**La solution est développée dans les règles de l'art :**
			P2B.1.6.1 Le développement répond à l'expression des besoins fonctionnels et respecte les contraintes techniques figurant dans le cahier des charges ;
B2B.1.10	Rédiger des documentations technique et d'utilisation d'une solution applicative		P2B.1.6.2 Les tests d'intégration sont réalisés ; P2B.1.6.3 Un outil collaboratif de gestion des itérations de développement et de versions est utilisé ; P2B.1.6.4 Une documentation des versions vient appuyer l'intégration continue ;
			P2B.1.6.5 Les composants logiciels sont documentés de manière à être réutilisés ;
B2B.1.11	Exploiter les fonctionnalités d'un environnement de développement et de tests		P2B.1.6.6 Un document est rédigé pour chaque contexte d'utilisation de l'application et est adapté à chaque destinataire tant par son contenu que par sa présentation ;
			P2B.1.6.7 Le développement tient compte des préoccupations de développement durable.
		P2B.1.7	L'application développée est opérationnelle conformément au cahier des charges et stable dans l'environnement de production.
B2B.2	**Assurer la maintenance corrective ou évolutive d'une solution applicative**	**B2B.2**	**Assurer la maintenance corrective ou évolutive d'une solution applicative**
B2B.2.1	Recueillir, analyser et mettre à jour les informations sur une version d'une solution applicative	P2B.2.1	L'évolution de la solution applicative répond aux besoins exprimés dans le cahier des charges.
B2B.2.2	Évaluer la qualité d'une solution applicative		
B2B.2.3	Analyser et corriger un dysfonctionnement	P2B.2.2	La modélisation de l'application existante est mise à jour par les nouvelles fonctionnalités et/ou les nouveaux correctifs apportés.
		P2B.2.3	L'interface utilisateur est mise à jour en respectant les contraintes ergonomiques.
		P2B.2.4	Un outil collaboratif de gestion des versions est utilisé.
		P2B.2.5	Des composants logiciels sont adaptés pour améliorer la qualité de la solution applicative.
		P2B.2.6	Les composants logiciels adaptés et/ou corrigés sont validés par les procédures de tests unitaires et fonctionnels.
		P2B.2.7	Le dysfonctionnement de la solution existante est corrigé selon les procédures en vigueur et dans les délais.
		P2B.2.8	Les accès aux données persistantes à travers le langage de requête du système de gestion de base de données relationnel, le langage de requête proposé par les échanges applicatifs des technologies Web, le langage de requête de l'outil de correspondance objet-relationnel ou toute autre solution de persistance sont mis à jour.
B2B.2.4	Mettre à jour des documentations technique et d'utilisation d'une solution applicative	P2B.2.9	Les tests de non régression sont réalisés.
		P2B.2.10	Les composants logiciels sont documentés de manière à être réutilisés.
		P2B.2.11	La documentation technique et d'utilisateurs de la solution applicative sont mises à jour.
B2B.2.5	Élaborer et réaliser les tests des éléments mis à jour	P2B.2.12	L'application améliorée et/ou corrigée est opérationnelle et stable dans l'environnement de production.
B2B.3	**Gérer les données**	**B2B.3**	**Gérer les données**
B2B.3.1	Exploiter des données à l'aide d'un langage de requêtes	P2B.3.1	L'exploitation des données permet de construire l'information attendue.
B2B.3.2	Développer des fonctionnalités applicatives au sein d'un système de gestion de base de données (relationnel ou non)	P2B.3.2	Les accès aux données sont contrôlés conformément aux habilitations définies par le cahier des charges.
		P2B.3.3	Les traitements pris en charge par les composants développés dans la base de données sont conformes aux demandes du cahier des charges.
B2B.3.3	Concevoir ou adapter une base de données	P2B.3.4	Les données sont modélisées conformément au besoin de la solution applicative.
		P2B.3.5	Le choix du type de base de données est pertinent.
		P2B.3.6	L'accessibilité des données est conforme à la qualité de service attendue.
B2B.3.4	Administrer et déployer une base de données	P2B.3.7	La base de données est sauvegardée selon la planification retenue.
		P2B.3.8	Des tests de restauration sont effectués.
		P2B.3.9	La base de données est opérationnelle et stable dans l'environnement de production.

Compétences / Performances BLOC3			
BLOC3	**Cybersécurité des services informatiques**	**BLOC3**	**Cybersécurité des services informatiques**
B3.1	**Protéger les données à caractère personnel**	**B3.1**	**Protéger les données à caractère personnel**
B3.1.1	Recenser les traitements sur les données à caractère personnel au sein de l'organisation	P3.1.1	La collecte, le traitement et la conservation des données à caractère personnel sont effectués conformément à la réglementation en vigueur.
B3.1.2	Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel	P3.1.2	La charte informatique contient des dispositions destinées à protéger les données à caractère personnel.
		P3.1.3	Des supports de communication pertinents sont accessibles et adaptés aux utilisateurs.
B3.1.3	Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel	P3.1.4	Le recensement des traitements des données à caractère personnel est exhaustif.
B3.1.4	Sensibiliser les utilisateurs à la protection des données à caractère personnel	P3.1.5	Des moyens de protection sont mis en place pour garantir la confidentialité et l'intégrité des données à caractère personnel en tenant compte des risques identifiés.
B3.2	**Préserver l'identité numérique de l'organisation**	**B3.2**	**Préserver l'identité numérique de l'organisation**
B3.2.1	Protéger l'identité numérique d'une organisation	P3.2.1	L'identité numérique de l'organisation est protégée en s'appuyant sur des moyens techniques et juridiques.
B3.2.2	Déployer les moyens appropriés de preuve électronique	P3.2.2	La preuve électronique est déployée de manière sécurisée et dans le respect de la législation.
B3.3	**Sécuriser les équipements et les usages des utilisateurs**	**B3.3**	**Sécuriser les équipements et les usages des utilisateurs**
B3.3.1	Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter	P3.3.1	Des supports de communication interne sont accessibles aux utilisateurs et adaptés à leurs destinataires.
B3.3.2	Identifier les menaces et mettre en œuvre les défenses appropriées	P3.3.2	**Les outils de défense mis en œuvre permettent de prévenir les menaces identifiées :**
			P3.3.2.1 L'accès physique au terminal et à ses données est sécurisé ;
			P3.3.2.2 Les applications installées sont vérifiées par des procédures automatisées et des logiciels de sécurité ;
			P3.3.2.3 Les flux réseaux sont identifiés et sécurisés.
B3.3.3	Gérer les accès et les privilèges appropriés	P3.3.3	**Les accès et privilèges respectent les règles organisationnelles :**
			P3.3.3.1 Les utilisateurs sont authentifiés ;
			P3.3.3.2 Les habilitations sont configurées ;
			P3.3.3.3 L'accès aux données est contrôlé ;
			P3.3.3.4 Les privilèges sont restreints.
B3.3.4	Vérifier l'efficacité de la protection	P3.3.4	L'efficacité de la protection mise en œuvre est évaluée.
B3.4	**Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberat - taques**	**B3.4**	**Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques**
B3.4.1	Caractériser les risques liés à l'utilisation malveillante d'un service informatique	P3.4.1	Les risques associés à l'utilisation malveillante d'un service informatique sont caractérisés.
B3.4.2	Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité	P3.4.2	Les conséquences des actes malveillants sur un service informatique sont identifiées.
B3.4.3	Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation	P3.4.3	Les obligations légales en matière d'archivage et de protection des données sont identifiées et respectées.
B3.4.4	Organiser la collecte et la conservation des preuves numériques	P3.4.4	Les preuves numériques sont conservées de manière sécurisée et dans le respect de la législation.
B3.4.5	Appliquer les procédures garantissant le respect des obligations légales	P3.4.5	**Des procédures garantissant le respect des obligations légales sont opérationnelles et appliquées :**
			P3.4.5.1 Un schéma présentant la segmentation du réseau est disponible ;
			P3.4.5.2 Les principes de mise en œuvre des contrôles des connexions aux réseaux sont validés ;
			P3.4.5.3 L'authentification et la confidentialité des échanges sont vérifiées ;
			P3.4.5.4 La sécurité de l'administration est prise en compte ;
			P3.4.5.5 Les accès physiques et logiques à un serveur ou à un service sont vérifiés en fonction des habilitations et des privilèges définis ;
			P3.4.5.6 Les accès aux données sont contrôlés à chaque étape d'une transaction ;
			P3.4.5.7 Les systèmes et les applications sont actualisés en fonction des alertes de sécurité ;
			P3.4.5.8 Les vulnérabilités connues sont contrôlées
B3.5	**Assurer la cybersécurité d'une solution applicative et de son développement**	**B3.5**	**Assurer la cybersécurité d'une solution applicative et de son développement**
B3.5.1	Participer à la vérification des éléments contribuant à la qualité d'un développement informatique	P3.5.1	Le respect des bonnes pratiques de développement informatique est vérifié (les structures de données sont normalisées, les accès aux données sont optimisés, le code est modulaire et robuste, les tests sont effectués).
B3.5.2	Prendre en compte la sécurité dans un projet de développement d'une solution applicative	P3.5.2	Les préoccupations de sécurité sont prises en compte à toutes les étapes d'un développement informatique.
B3.5.3	Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité	P3.5.3	Les bonnes pratiques de sécurité sont mises en œuvre à toutes les étapes d'un développement informatique.
B3.5.4	Prévenir les attaques	P3.5.4	Des tests de sécurité sont prévus et mis en œuvre.
B3.5.5	Analyser les connexions (logs)	P3.5.5	Les traitements sur les données à caractère personnel sont déclarés et respectent la réglementation.
		P3.5.6	Le système d'authentification est conforme aux règles de sécurité.
		P3.5.7	L'accès aux données respecte les règles de sécurité.
		P3.5.8	Les échanges de données entre applications sont protégés.
		P3.5.9	Les composants utilisés sont certifiés, sécurisés et actualisés.
B3.4.6	Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures	P3.5.10	Les contre-mesures mises en place corrigent et préviennent les incidents de sécurité.
		P3.5.11	Les contre-mesures sont documentées de manière à en assurer le suivi.
		P3.5.12	La communication écrite et orale est adaptée à l'interlocuteur.