ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

RÉFÉRENTIEL D'ACTIVITÉS, DE COMPÉTENCES ET D'ÉVALUATION

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 1 : **Manager les équipes et la transformation du SI**			
A1.1 Encadrer les équipes internes et/ou externes	C1.1.1 Gérer et encadrer son équipe (responsabilité hiérarchique) pour développer les compétences et optimiser l'organisation du système d'information en s'assurant que les tâches affectées soient accessibles et en cohérence avec les compétences des membres de l'équipe C1.1.2 Organiser et piloter une équipe (responsabilité fonctionnelle) pour optimiser la réalisation des projets IT en utilisant des outils collaboratifs et en adaptant son style de management C1.1.3 Manager les relations clients/fournisseurs pour optimiser la mise en œuvre des projets IT en utilisant les moyens de communications et les outils collaboratifs adaptés et accessibles	**E1. Épreuve écrite et orale** : Application professionnelle (réelle ou simulée) de management de la transformation du SI, le candidat produit un document professionnel qui comprend : - La présentation de l'entreprise et du SI existant - La présentation des évolutions du SI - L'organigramme de l'équipe projet - Le plan de communication et les outils utilisés dans la gestion de la relation des prestataires ou fournisseurs. - Les outils collaboratifs sélectionnés pour le projet. - La méthode et le plan d'accompagnement du changement) Suivi d'une présentation orale devant le jury	Cr1.1.1 Les responsabilités et les affectations de l'équipe projet opérationnelle sont clairement exprimées. Les responsabilités sont cohérentes avec les tâches à réaliser dans le projet et vis-à-vis des compétences individuelles. Cr1.1.2 Un organigramme de l'équipe projet est présenté avec une affectation pertinente des tâches. Le type de management mis en œuvre est adapté et les outils de suivi servent les objectifs du projet et optimisent le fonctionnement de l'équipe projet. Cr1.1.3 Les fournisseurs et sous-traitants sont identifiés. Un plan de communication utilisant des outils collaboratifs et accessibles est proposé.
A1.2 Modéliser les flux métiers et les ressources techniques du SI (acteurs, flux d'information, étapes, etc.) en intégrant le contexte existant	C1.2.1 Analyser l'environnement technique et métier utilisant le système d'information pour en identifier les processus, les workflows et les technologies existantes en exploitant les données disponibles (documentations techniques, rapports d'activités, audits, interviews, etc.) C1.2.2 Modéliser le SI en synthétisant les données utiles pour le rendre compréhensible par les décideurs C1.2.3 Identifier les améliorations possibles du SI pour optimiser les flux métiers en répondant aux enjeux stratégiques de l'entreprise		Cr1.2.1 La présentation de l'entreprise et de son activité est exhaustive et claire. Elle intègre les processus de l'entreprise, les workflows des flux d'information. Cr1.2.2 La présentation du SI existant est claire et représentée graphiquement (topologies réseau, systèmes, données, applications). Cr1.2.3 Au moins 5 axes d'amélioration possibles des flux du SI sont identifiés sur les aspects applicatifs, réseau, stockage, hébergement, accès utilisateurs, etc. Ils répondent aux enjeux de l'entreprise.
A1.3 Conduire le changement induit par les projets de la DSI	C1.3.1 Identifier une méthode de gestion du changement pour garantir l'adhésion des parties prenantes en s'appuyant sur les leviers de motivation et d'engagement identifiés C1.3.2 Définir et conduire le plan d'accompagnement en identifiant les acteurs et les actions à mener (formation, communication, régulation, mesure, etc.) pour s'assurer de l'appropriation par tous de la transformation induite par la stratégie de la DSI		Cr1.3.1 La méthode choisie et les leviers de motivation et d'engagement trouvés sont cohérents pour faire adhérer au projet, les arguments sont efficaces et convaincants. Cr1.3.2 Les acteurs clés du projet sont listés. Les moyens de communication adaptés aux parties prenantes sont identifiés et pertinents.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 2 : **Superviser le portefeuille projets de la DSI et sa mise en œuvre**			
A2.1 Définir, prioriser et faire vivre le portefeuille de projets	C2.1.1 Élaborer le référentiel documentaire des projets IT afin de garantir son appropriation par les acteurs des projets et d'harmoniser la formalisation et la gestion des projets (réception de la demande, analyse de faisabilité, etc.) en se basant sur les pratiques de l'entreprise et les référentiels existants (méthodologies de type cycle en V, méthodologies agiles, etc.) C2.1.2 Définir des critères de choix pertinents pour gérer les priorités du portefeuille projets du SI et ordonnancer l'ensemble des projets proposés en tenant compte des règles applicables (législatives, normatives, culturelles, éthiques, etc.) C2.1.3 Exposer et défendre les choix effectués pour permettre une lecture claire et cohérente auprès des hiérarchiques et des fonctionnels lors de la sélection des projets informatiques grâce à une présentation des cotations réalisées	**E2 Épreuve écrite** : Application professionnelle (réelle ou simulée) sur la supervision d'un portefeuille projets, le candidat produit un document professionnel qui comprend : - Le référentiel documentaire des projets - Les tableaux de bord de gestion du portefeuille de projets - Le plan de management de l'un des projets - Le tableau de bord de suivi de projet - Le plan de test et le cahier de recette - Le PV de recette - Le résultat de la capitalisation	Cr2.1.1 Le référentiel documentaire des projets comprend à minima les modèles de charte de projet, cahier des charges, budget, planning, gestion des risques. Chaque modèle est établi selon l'état de l'art et formalisé dans le respect de la charte graphique de l'entreprise. Cr2.1.2 Les critères de choix proposés sont cohérents avec la stratégie SI de l'entreprise, elle-même clairement exposée. Cr2.1.3 Les cotations sont effectuées de façon factuelle. Elles permettent d'argumenter le choix des projets et leur priorité.
A2.2 Superviser et conduire les projets IT	C2.2.1 S'approprier le contexte et le périmètre de chaque projet IT en identifiant ses objectifs, ses enjeux et ses contraintes spécifiés afin d'apporter une réponse au besoin exprimé par la maîtrise d'ouvrage C2.2.2 Établir le plan de management (gestion des risques, planification, organisation, budget, indicateurs, parties prenantes, plan de communication, etc.) de chaque projet IT à conduire afin de pouvoir en suivre l'avancée en s'appuyant sur les outils de management de projet C2.2.3 Contrôler et valider les différents livrables des projets IT pour respecter le triangle d'or (qualité, coût, délai) attendu en mettant à jour les tableaux de bord de suivi du projet		Cr2.2.1 Les objectifs, les enjeux et les contraintes du projet sont clairement identifiés. Ils sont pris en compte dans le plan de management (respect des livrables et des échéances souhaitées). Cr2.2.2 Le plan de management proposé comprend à minima la charte de projet, le cahier des charges fonctionnel (ou backlog[1]), le budget, le planning, la gestion des risques et le plan de communication. Il permet de répondre aux objectifs du projet. Cr2.2.3 Les indicateurs et les outils de suivi identifiés permettent de respecter les attendus du projet.
A2.3 Clore les projets et capitaliser l'expérience	C2.3.1 Organiser les recettes (fonctionnelle et technique) de chaque projet IT pour livrer un produit conforme aux exigences du client en établissant les cahiers de recette C2.3.2 Établir les documents administratifs, contractuels et techniques des projets IT (solde des contrats, procès-verbaux de recette, documentations techniques, etc.) pour formaliser la clôture du projet dans le respect des règlements en vigueur (RGPD, droit commercial, etc.) et aux exigences fonctionnelles et techniques C2.3.3 Organiser et animer la capitalisation de l'expérience à l'issue des projets IT au sein des équipes projet (réunions, documentation, etc.) en analysant les indicateurs de performance du projet (État d'avancement, économie réalisée, avancée technique, etc.) dans un objectif d'amélioration continue		Cr2.3.1 Le plan de test présenté est exhaustif. Il permet de valider toutes les étapes du projet. Cr2.3.2 Le procès-verbal de recette présenté permet de répondre à l'ensemble des fonctionnalités attendues et de garantir la qualité des livrables en tenant compte des référentiels en vigueur. Cr2.3.3 Les outils de capitalisation d'expérience mis en place ont permis d'identifier des améliorations pertinentes (révision du référentiel documentaire, méthode de gestion de projet, canaux de communication, etc.) pour le pilotage des futurs projets SI.

[1] Backlog : liste de cas d'usages

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 3 : **Concevoir l'infrastructure du système d'Information**			
A3.1 Auditer les infrastructures existantes et analyser les solutions réseaux, data et cloud du marché	C3.1.1 Auditer l'infrastructure du SI pour identifier les limites et points faibles en vérifiant la conformité par rapport aux standards technologiques, organisationnels et de cybersécurité (Préconisation ANSSI et principaux éditeurs) C3.1.2 Étudier et comparer les différentes solutions technologiques afin de réaliser les choix adaptés aux besoins métiers de l'entreprise	**E3 Épreuve orale** : Application professionnelle (réelle ou simulée) sur la conception d'une infrastructure informatique sécurisée, le candidat présente devant le jury : - Le résultat d'audit et l'analyse des services ou éléments du SI nécessitants une évolution - La présentation de la nouvelle architecture comprenant le comparatif des offres - La liste des projets priorisés pour mettre en œuvre la nouvelle infrastructure - La bibliographie / webographie de la veille technique - Les indicateurs de suivi de l'activité des services et des technologies	Cr3.1.1 L'audit couvre à minima l'infrastructure système, réseau et le stockage des données. Les différents éléments et/ou services nécessitant une évolution sont identifiés. Cr3.1.2 Le comparatif des solutions traite les grands éditeurs de solutions système, réseaux et cloud (Amazon, Microsoft, Google, etc.). Il comprend à minima prix, fonctionnalités, niveau de sécurité garanti, niveau de disponibilité.
A3.2 Concevoir une infrastructure informatique sécurisée (réseaux, data, systèmes, cloud, etc...)	C3.2.1 Concevoir une infrastructure informatique sécurisée (réseaux, cloud, ERP, data, sauvegarde, etc.) en s'appuyant sur les besoins clients, les standards d'architecture des SI[2] et les bonnes pratiques en terme de cybersécurité C3.2.2 Identifier les projets qui composeront le portefeuille projet d'évolution et de migration de l'architecture du SI		Cr3.2.1 La nouvelle infrastructure est présentée sous forme de topologie et répond aux besoins du client. Les flux de données sont représentés et les solutions techniques choisies traitant au moins des aspects système, réseau, cloud et stockage, sont argumentées. Cr3.2.2 Les projets à réaliser sont identifiés. Ils sont en cohérence avec l'architecture choisie (Systèmes, Réseau, Cloud, Stockage). Ils sont priorisés selon les exigences techniques.
A3.3 Conseiller les décideurs sur la gouvernance de l'infrastructure du SI	C3.3.1 Organiser et animer un système de veille active sur les technologies des SI et les menaces en cybersécurité en s'informant auprès des éditeurs, prestataires et organismes de référence de type ANSSI C3.3.2 Analyser les solutions implantées pour identifier les besoins de mises à jour ou d'évolutions du SI en définissant des indicateurs d'activité ou de détection de problèmes de sécurité C3.3.3 Conseiller la direction sur les projets et investissements à conduire pour aider à la prise de décision et à la gouvernance du SI en présentant des indicateurs formalisés sous forme de tableaux de bord par exemple		Cr3.3.1 La veille professionnelle mise en place est exhaustive et récente. Elle sert les enjeux du système d'information de l'entreprise et permet d'adapter les solutions techniques. Cr3.3.2 Au moins 3 indicateurs choisis permettent de répondre au besoin de la veille sur l'activité du SI. Cr3.3.3 Au moins 3 indicateurs cohérents avec le contexte de l'entreprises permettent la prise de décision pour un maintien ou une évolution des solutions choisies. Ils sont présentés dans un tableau de bord synthétique et visuel.

[2] Systèmes d'Information

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 4 : **Sécuriser les infrastructures du système d'Information (accès, réseaux et données)**			
A4.1 Organiser l'analyse et la surveillance des menaces en cybersécurité	C4.1.1 Auditer l'infrastructure du SI afin d'identifier les éléments nécessitant une sécurisation ainsi que le niveau de sécurité nécessaire (accès, données, etc.) en utilisant des outils de pentesting[3] associés à une méthodologie d'audit C4.1.2 Identifier les droits, les obligations et normes applicables en matière de sécurisation du SI afin de garantir sa conformité réglementaire et normative en s'appuyant sur les standards et normes relatives à la cybersécurité (RGPD, ISO27001, CNIL, etc.)	**E4 Épreuve écrite** : Application professionnelle (réelle ou simulée) sur la sécurisation d'une infrastructure informatique, le candidat produit un document professionnel qui comprend : - Le résultat d'audit et l'analyse du niveau de sécurisation du SI - Les normes et règlementations en vigueur - Un plan de remédiation - La bibliographie / webographie de la veille cybersécurité et des menaces existantes - Les indicateurs de pilotage de la sécurité du SI - Un plan de gestion de crise et ses préconisations - Les Outils de détection configurés - La procédure de restauration / rétablissement du service	Cr4.1.1 L'audit sécurité du SI est complet et méthodique. Il permet d'identifier les failles de sécurité et les menaces qu'encoure le SI. Il s'appuie sur une des méthodologies d'audit existantes (COBIT, ISO27002, etc.). Cr4.1.2 Les droits, normes et obligations applicables sont identifiés de façon exhaustive. Leur analyse permet d'établir un plan de mise en conformité de la gestion de la sécurité du SI particulièrement en terme d'accès, de gestion des données et de traçabilité.
A4.2 Concevoir et piloter les solutions de sécurisation du système d'information	C4.2.1 Concevoir le plan de sécurisation et de supervision du SI pour répondre au niveau de sécurisation attendu en s'appuyant sur les résultats de l'audit et dans le respect des obligations règlementaires et normatives (RGPD, CNIL, etc.) ainsi que sur les bonnes pratiques de sécurisation des SI C4.2.2 Identifier les opérations et les parties prenantes pour organiser et planifier les projets de sécurisation du SI en s'appuyant sur une méthodologie de gestion de projet de type AGILE C4.2.3 Suivre et superviser la mise en œuvre des solutions de sécurisation pour mesurer leur efficacité et garantir le niveau de sécurisation requis en définissant des indicateurs de suivis appropriés et des outils de surveillance de type SIEM[4]		Cr4.2.1 Le plan de sécurisation présenté répond aux exigences règlementaires. Il propose les contre-mesures nécessaires suite aux écarts et risques identifiés. Il comprend des outils de supervision (sécurisation des accès, du réseau, des données, supervision de type SIEM, etc.). Cr4.2.2 Les opérations, projets et préconisations de sécurisation sont identifiés de façon claire et exhaustive. Les ressources nécessaires sont listées et adaptées au besoin. L'organisation proposée est cohérente avec le projet de sécurisation du SI. Cr4.2.3 Au moins 3 indicateurs de suivi sont présentés de façon synthétique et visuelle dans un tableau de bord. Ils permettent de maintenir efficacement le niveau de sécurité exigé.

[3] Test de pénétration
[4] Security Information and Event Management

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
BLOC 4 : **Sécuriser les infrastructures du système d'Information (accès, réseaux et données)**			
A4.3 Conseiller les décideurs sur la politique de sécurisation du SI	C4.3.1 Organiser et animer un système de veille active pour se tenir à jour sur les menaces en cybersécurité et solutions de sécurisation en s'informant auprès des éditeurs, prestataires et organismes de référence (ANSSI, CERT, etc.) C4.3.2 Analyser les indicateurs d'activité pour identifier les besoins de mises à jour, évolutions ou failles de sécurité en s'appuyant sur les informations de veille C4.3.3 Conseiller la direction sur les projets et investissements à conduire en terme de cybersécurité et aider à la mise en œuvre d'une gouvernance de la sécurité SI en présentant des indicateurs formalisés sous forme de tableaux de bord par exemple	**E4 Épreuve écrite** (suite) : Application professionnelle (réelle ou simulée) sur la sécurisation d'une infrastructure informatique, le candidat produit un document professionnel qui comprend : - Le résultat d'audit et l'analyse du niveau de sécurisation du SI - Les normes et règlementations en vigueur - Un plan de remédiation - La bibliographie / webographie de la veille cybersécurité et des menaces existantes - Les indicateurs de pilotage de la sécurité du SI - Un plan de gestion de crise et ses préconisations - Les Outils de détection configurés - La procédure de restauration / rétablissement du service	Cr4.3.1 L'organisation de la veille professionnelle est présentée sous la forme d'une liste de sources et modalités d'accès à l'information. Le plan d'audit comprend les types d'audits à réaliser ainsi que la fréquence et les parties prenantes. Les informations fournies servent les enjeux du système d'information de l'entreprise et permettent d'adapter le niveau de sécurisation du SI. Cr4.3.2 Les indicateurs choisis et les outils de supervisions sont adaptés et répondent au besoin de veille sur le niveau de sécurité du SI. Cr4.3.3 Les indicateur sont pertinents et synthétiques, ils permettent la prise de décision pour un maintien ou une évolution des solutions de sécurisation choisies.
A4.4 Gérer une crise en cybersécurité	C4.4.1 Anticiper la crise cyber pour réagir rapidement et gérer ses impacts en mettant en place une évaluation des risques, un plan de continuité d'activité, un plan de communication et une identification des rôles et responsabilités C4.4.2 Détecter et identifier l'attaque pour adapter la réponse en analysant les données de surveillance et les incidents de sécurité C4.4.3 Gérer l'incident et répondre à la crise pour stopper sa progression et rétablir un système d'information sain en rendant le plan de communication accessible à tous les acteurs internes et externes et en activant les solutions de restauration C4.4.4 Évaluer les dommages pour améliorer la résilience du SI en analysant l'attaque, les pertes subies et en mettant à jour les solutions techniques et le plan de crise cyber		Cr4.4.1 Le plan de communication et le plan de continuité d'activité sont cohérents avec le type de crise cyber traité. Le rôles et responsabilités des différents acteurs sont établis dans un document synthétique et accessible. Cr4.4.2 Au moins deux outils de détection et de surveillance sont proposés. Ils sont adaptés aux menaces. Leur configuration est cohérente avec les menaces et les impacts sur le SI. Cr4.4.3 Au moins une contre mesure adaptée à l'incident est mise en œuvre. La procédure de restauration et/ou de rétablissement cohérente avec le type de crise cyber traité et le systèmes d'information. Cr4.4.4 Au moins deux axes de renforcement (Plan de communication, outils, système de restauration, etc.) du SI sont proposés. Ils permettent l'amélioration de la résilience du SI.

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

Pour viser la certification professionnelle complète « Manager en infrastructures et cybersécurité des systèmes d'information », le candidat doit :
- Valider les 4 blocs ci-dessous
- Se présenter à un grand oral devant un jury de professionnels, -*Voir Note pédagogique du grand oral de niveau 7 en pièce complémentaire au dossier, rubrique Autres pièces nécessaires-,*
- Réaliser une période d'application en entreprise de 6 mois consécutifs ou non.

Liste des blocs de compétences :
- Bloc 1 : Manager les équipes et la transformation du SI
- Bloc 2 : Superviser le portefeuille projets de la DSI et sa mise en œuvre
- Bloc 3 : Concevoir l'infrastructure du système d'information
- Bloc 4 : Sécuriser les infrastructures du système d'information (accès, réseaux et données)