

ERIS - Expert réseaux infrastructures et sécurité – niveau 7



Article L6113-1 - Créé par LOI n°2018-771 du 5 septembre 2018 - art. 31 (V) "Les certifications professionnelles enregistrées au répertoire national des certifications professionnelles permettent une validation des compétences et des connaissances acquises nécessaires à l'exercice d'activités professionnelles. Elles sont définies notamment par un référentiel d'activités qui décrit les situations de travail et les activités exercées, les métiers ou emplois visés, un référentiel de compétences qui identifie les compétences et les connaissances, y compris transversales, qui en découlent et un référentiel d'évaluation qui définit les critères et les modalités d'évaluation des acquis."

Prérequis à l'entrée en formation : être titulaire d'une certification de niveau 6 dans le domaine de l'administration systèmes et réseaux.

Code NSF :

326 : Informatique, traitement de l'information, réseaux de transmission

326n : Analyse informatique, conception d'architecture de réseaux

Disposition pour les modalités d'évaluation pour les PSH : Avant le début de son cursus le candidat est reçu individuellement et pris en charge par le Référent Handicap de l'école afin de faire un point très précis sur ses besoins et ce qui était déjà mis en place précédemment dans son parcours. Le référent handicap est chargé de mettre en place un 1/3 temps pour les évaluations, de mettre à disposition une salle dédiée avec à disposition un paperboard, des copies adaptées au format spécifique pré-quadrillé facilitant leur utilisation, une salle dans laquelle le candidat peut s'isoler (lumière tamisée, climat calme et serein). Pour des candidats ne pouvant s'exprimer lors des épreuves orales, des modalités d'échange textuelles, avec un jury averti et un accompagnateur/traducteur, sont organisées et autorisées si la situation le nécessite. Dans tous les cas, l'équipe pédagogique est informée. Le respect du principe d'anonymat s'applique pour les copies et corrigées exactement dans les mêmes conditions que les autres copies.

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p>A1 – Gouvernance des infrastructures Systèmes et Réseaux</p> <p>A1.1 – Participation à la définition des politiques de gouvernance de l'infrastructure</p> <p><i>L'expert ERIS définit les politiques de gouvernance de l'infrastructure ou participe à leur définition dans le cadre de la DSI¹ en se basant sur les bonnes pratiques telles que ITIL² et COBIT³. Il intègre des référentiels comme ISO 2700x pour la sécurité des systèmes d'information, garantissant une gestion structurée des services IT.</i></p> <p><i>Il participe à la prise de décision quant au traitement interne ou externe du projet et assure le cas échéant la sélection et le suivi de la prestation.</i></p>	<p>C01 - Participer aux politiques de gouvernance IT dans le cadre du schéma directeur de la DSI, en s'appuyant sur des référentiels de bonnes pratiques, en mobilisant son expertise technique, et en contribuant à la structuration de la gestion des services IT, pour garantir que la gestion l'infrastructure répondent aux exigences de performance, de sécurité et de conformité.</p>	<p>Évaluation n°1 : mise en situation professionnelle simulée à partir d'un scénario d'entreprise fictive dont il faut gérer les services informatiques.</p> <p>Préparation collective des livrables écrits et oral individuel (Compétences C01 à C10)</p>	<p>Cr01.1 - Les politiques de gouvernance définies permettent d'assurer la cohérence et l'homogénéité des pratiques.</p> <p>Cr01.2 - Les politiques de gouvernance définies s'inscrivent dans le cadre du schéma directeur de la DSI.</p> <p>Cr01.3 - Les politiques de gouvernance permettent à l'entreprise d'atteindre ses objectifs en matière de performance, sécurité et conformité.</p>

¹ DSI : Direction des Systèmes d'Information

² ITIL : Information Technology Infrastructure Library

³ COBIT : Control Objectives for Information and related Technology

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p>A1.2 – Contrôle de la conformité réglementaire</p> <p><i>L'expert ERIS est souvent actif au sein d'une DSI⁴. Il travaille en étroite collaboration avec les instances dirigeantes, les comités de pilotage, et les départements juridiques et de conformité pour s'assurer de la conformité avec les réglementations telles que le RGPD, ISO 2700x, ainsi que les directives NIS2 pour la sécurité des systèmes d'information. Il s'appuie sur les recommandations de l'ANSSI⁵ et de la CNIL.</i></p> <p><i>Il veille à ce que les infrastructures soient conformes aux normes de l'entreprise et aux réglementations en effectuant des audits.</i></p>	<p>C02 - Auditer l'infrastructure de l'entreprise en évaluant systématiquement les volets techniques et organisationnels à l'aide de méthodes d'analyse, d'outils de surveillance et de cadres de référence pour contrôler la conformité réglementaire.</p>		<p>Cr02.1 - L'audit couvre les volets techniques et organisationnels.</p> <p>Cr02.2 - L'audit précise les éléments contrôlés, les mesures à effectuer et les valeurs cibles.</p> <p>Cr02.3 - Toutes les normes et réglementations retenues par l'entreprise sont prises en compte.</p>
<p>A1.3 – Gestion des contrats de services ou SLA (Service Level Agreements)</p> <p><i>L'expert ERIS négocie, établit et gère les accords de niveau de service (SLA) pour garantir que les prestations ou que les réalisations répondent aux attentes des clients internes et externes.</i></p> <p><i>Il définit des indicateurs de performance (KPI) pour mesurer le respect des SLA, met en place des processus (au sens ISO) et utilise des outils</i></p>	<p>C03 - Etablir des accords de niveaux de service (SLA) en collaboration avec les clients internes et/ou externes, en définissant des indicateurs clés de performance (KPI) et leurs valeurs cibles associées, réunis en tableaux de bord et en utilisant des outils de gestion de SLA, afin d'offrir des prestations ou des réalisations répondant aux exigences et objectifs de l'entreprise.</p>		<p>Cr03.1 - Les accords de niveau de service proposés permettent à l'entreprise d'atteindre ses objectifs et niveaux d'exigence fixés.</p> <p>Cr03.2 - Les indicateurs clés de performance choisis permettent de mesurer le respect des SLA.</p> <p>Cr03.3 - Les valeurs cibles associées sont en accord avec les niveaux d'exigence</p>

⁴ DSI : Direction du Système d'Information

⁵ ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p><i>de gestion des SLA pour surveiller et rapporter la performance des services.</i></p> <p><i>En cas de non-respect des SLA, il analyse les causes et propose des actions correctives.</i></p> <p><i>L'expert ERIS réalise des audits réguliers des services pour assurer leur efficacité et conformité en utilisant les indicateurs de performance (KPI), en s'appuyant sur des outils tels que CISA et ACL Analytics pour mener à bien ces audits.</i></p> <p><i>Il développe des rapports périodiques détaillés et des tableaux de bord et propose des améliorations.</i></p>	<p>C04 - Elaborer, documenter et mettre en œuvre des processus et procédures standardisées en s'appuyant sur des normes et/ou référentiels tels que ISO 9001 et ITIL pour garantir la qualité et l'efficacité des services.</p> <p>C05 - Analyser les causes de non-respect des SLA en s'appuyant sur les KPI et des outils d'audit et d'analyse de données afin de proposer des actions correctives.</p>		<p>Cr04.1 - Les processus et procédures sont documentés et s'appuient sur des normes et/ou référentiels de bonnes pratiques.</p> <p>Cr04.2 - Les processus et procédures définis permettent d'atteindre le niveau de qualité et d'efficacité des services souhaité.</p> <p>Cr05.1 - La méthodologie suivie pour interpréter les données et les KPI permet d'identifier les causes de non-respect des SLA.</p> <p>Cr05.2 - Les actions correctives proposées permettent de se replacer dans le contexte de respect des SLA.</p>
<p>A1.4 – Mise en œuvre des Plans de Continuité (PCA) et de Reprise d'Activité (PRA)</p> <p><i>L'expert ERIS développe et met en œuvre des plans de continuité d'activité (PCA) pour garantir les engagements de services (SLA) et de reprise d'activité (PRA) pour garantir la résilience des systèmes en cas de sinistre.</i></p> <p><i>Il identifie les processus critiques et les ressources nécessaires pour maintenir ou restaurer les opérations.</i></p>	<p>C06 - Evaluer les risques pesant sur la production en lien avec l'informatique, en identifiant les menaces, en évaluant leurs probabilités et impacts afin de définir et documenter des plans de continuité et de reprise de l'activité.</p>		<p>Cr06.1 - L'analyse de risque couvre les processus critiques en lien avec l'informatique pour l'activité de l'entreprise.</p> <p>Cr06.2 - L'analyse de risque constitue une base suffisante pour définir des plans de continuité et de reprise d'activité.</p> <p>Cr06.3 - Chaque menace est correctement évaluée en termes de probabilité et impacts.</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p><i>Dans le cadre du PCA, il utilise des techniques de redondance afin d'atteindre le degré de Haute Disponibilité souhaité.</i></p> <p><i>Dans le cadre du PRA, il planifie et gère les sauvegardes et les restaurations des données pour minimiser les pertes et les interruptions en utilisant des outils tel que Veeam Backup.</i></p> <p><i>L'expert ERIS teste régulièrement les PCA et PRA à travers des simulations et des exercices pour s'assurer de leur efficacité et de la capacité des équipes à réagir.</i></p> <p><i>Il actualise les plans en fonction des évolutions technologiques et des menaces et risques émergents en collaborant avec les parties prenantes.</i></p>	<p>C07 - Elaborer un plan de continuité d'activité (PCA) en s'appuyant sur les SLA et l'analyse de risques, en produisant sa documentation et en définissant les moyens humains et techniques nécessaires à sa mise en place afin de respecter le niveau de service contractuel.</p>		<p>Cr07.1 - Le plan de continuité d'activité est en lien avec un risque clairement identifié et contribue au respect des SLA.</p> <p>Cr07.2 - Les moyens humains et techniques mobilisés sont en cohérence avec le contexte de l'entreprise et permettent d'atteindre l'objectif de façon optimisée.</p> <p>Cr07.3 - La documentation est complète et permet d'identifier les rôles et actions nécessaires à la mise en œuvre du plan.</p>
	<p>C08 - Définir un plan de reprise d'activité (PRA) en priorisant les applications et services critiques et en établissant des stratégies de sauvegarde, avec respect du principe du 3-2-1, et de restauration, aussi bien matérielle et/ou logicielle qu'organisationnelle, afin d'assurer une protection optimale contre les risques de perte de données, et permettre une récupération rapide et efficace en cas de sinistre.</p>		<p>Cr08.1 - L'ordre de priorisation des applications et services du plan de reprise d'activité est déterminé par leur degré de criticité par rapport aux activités de l'entreprise.</p> <p>Cr08.2 - Les stratégies de sauvegarde et de restauration s'appuient sur cet ordre et définissent les éléments techniques et organisationnels nécessaires.</p> <p>Cr08.3 - Le plan de reprise d'activité permet d'atteindre les objectifs de l'entreprise en termes de niveau de protection contre les risques de perte de données et d'efficacité de restauration.</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
	C09 - Etablir et mettre en œuvre des tests des plans de continuité (PCA) et des plans de reprise d'activité (PRA) en simulant des situations de crise réelles ou de pannes majeures sous forme d'exercices réflexifs, pratiques ou simulés afin d'améliorer la préparation aux incidents et assurer la résilience des infrastructures systèmes et réseaux.		Cr09.1 - Les exercices mis en place pour les tests permettent d'évaluer la viabilité du PCA ou PRA visé. Cr09.2 - Les observations et conclusions tirés des tests permettent une amélioration de la gestion des situations de crise.
A1.5 – Promotion et intégration du Numérique Responsable <i>L'expert ERIS met en œuvre des pratiques de numérique responsable en conformité avec les réglementations françaises et européennes telles que la loi REEN (Réglementation Écologique des Équipements Numériques), le RGESN (Référentiel Général d'Eco-conception des Services Numériques), et le RGAA (Référentiel Général d'Accessibilité pour les Administrations).</i> <i>Il développe des stratégies visant à réduire l'empreinte carbone des infrastructures IT, optimise la consommation énergétique des datacenters, et encourage une utilisation éthique et durable des outils informatiques.</i> <i>Il utilise les outils de référence (RGESN, REEN) pour mesurer et améliorer la performance environnementale du SI.</i>	C10 - Mettre en œuvre le Numérique Responsable en adaptant des pratiques durables et d'accessibilité (personnes en situation de handicap), en se basant sur l'inventaire exhaustif des actifs informatiques et en utilisant les outils de référence afin de mesurer et d'améliorer la performance environnementale du SI et les pratiques RSE afférentes.		Cr10.1 - L'inventaire des actifs informatiques est complet et permet de construire une mesure de performance environnementale fiable. Cr10.2 - Les pratiques mises en œuvre permettent d'atteindre les objectifs RSE et environnementales de l'entreprise. Cr10.3 - La conformité avec les réglementations en vigueur est assurée.

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p>A2 – Conception et Pilotage des Infrastructures Systèmes et Réseaux.</p> <p>A2.1 - Conception d'architectures systèmes et réseaux</p> <p><i>A partir de l'analyse des besoins métiers, l'expert ERIS conçoit des infrastructures sécurisées en anticipant l'évolution de ces derniers.</i></p> <p><i>Il intègre des solutions de gestion des identités (IAM) telles que Active Directory (AD), LDAP ou Azure AD, pour s'assurer que les bonnes personnes aient le bon niveau d'accès aux ressources.</i></p> <p><i>Il optimise l'utilisation des ressources en assurant la flexibilité et la scalabilité du système au moyen de technologies de virtualisation telles que VMware vSphere et Microsoft Hyper-V ainsi que de technologies de conteneurisation telles que Docker et Kubernetes.</i></p> <p><i>Il conçoit la topologie des réseaux de l'entreprise mono ou multisites (LAN, WAN, réseaux sans fils), en utilisant des équipements tels que Cisco, Aruba et Fortinet.</i></p> <p><i>Il intègre des systèmes de téléphonie sur IP (ToIP) tels que Cisco UC, Microsoft Teams et Asterisk, tout en garantissant la qualité de service (QoS) et la sécurité des communications.</i></p>	<p>C11 - Concevoir une infrastructure système et réseau optimisée et sécurisée en analysant les besoins métiers et en proposant des solutions, en conformité avec le schéma directeur de la DSI, en combinant des ressources locales (on-premise) et/ou Cloud (SaaS, PaaS, IaaS) afin de fournir une base technique robuste et efficace soutenant les opérations de l'entreprise tout en garantissant la sécurité des données et des communications.</p> <p>C12 - Définir, implémenter et contrôler les règles d'accès aux données et aux services en retranscrivant les règles métiers dans une solution de gestion des identités (IAM*) afin de protéger les systèmes et les données sensibles contre les accès non autorisés.</p>	<p>Evaluation n°2 : mise en situation professionnelle simulée de montage d'infrastructure.</p> <p>Epreuve pratique individuelle avec interrogation orale au fil de l'épreuve (Compétences C11 à C16)</p>	<p>Cr11.1 - Tous besoins métiers recensés sont couverts par l'infrastructure proposée.</p> <p>Cr11.2 - L'infrastructure proposée est conforme au schéma directeur de la DSI.</p> <p>Cr11.3 - L'infrastructure proposée répond aux exigences de l'entreprise en termes d'optimisation, de robustesse, et de sécurité.</p> <p>Cr12.1 - Les règles d'accès mises en place dans l'IAM sont conformes aux règles métiers de l'entreprise.</p> <p>Cr12.2 - Les contrôles effectués permettent de vérifier que les bonnes personnes ont le bon niveau d'accès aux ressources.</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p><i>Il conçoit également des infrastructures hybrides qui combinent des ressources on-premise (locales) et Cloud (SaaS, PaaS, IaaS), afin d'optimiser les coûts, la performance et la flexibilité. Pour cela, il s'appuie sur des plateformes telles que Amazon AWS, Microsoft Azure et Google Cloud Platform.</i></p>	<p>C13 - Arbitrer la technologie d'hébergement des systèmes et/ou applications (serveur dédié, virtualisation, conteneurisation/orchestration ou cloud) en évaluant et optimisant les ressources nécessaires à leur usage (telles que machine, stockage, bande passante, processeur, mémoire, consommation électrique), pour les déployer, les mettre en production et les gérer de manière fiable, flexible et scalable.</p> <p>C14 - Concevoir une topologie des réseaux de l'entreprise tant mono que multisites, en tenant compte des engagements de disponibilité, de capacité afin de garantir la qualité de service (QoS), la résilience (PCA) et la sécurité des communications.</p>		<p>Cr13.1 - Le type d'hébergement retenu permet de répondre aux critères métiers prévus (performance, fiabilité, flexibilité et scalabilité).</p> <p>Cr13.2 - La solution retenue prend en compte les ressources mobilisées pour chaque usage (machine, stockage, bande passante, processeurs, mémoire, consommation électrique etc.) et permet de les optimiser.</p> <p>Cr14.1 - La topologie proposée permet la mise en place des services nécessaires au bon fonctionnement de l'activité de l'entreprise.</p> <p>Cr14.2 - Les équipements retenus et leur implantation dans la topologie permettent d'atteindre les objectifs en matière de QoS, de résilience et de sécurité.</p>
<p>A2.2 - Gestion et Supervision de la Mise en Œuvre de l'Infrastructure (MOE)</p> <p><i>L'expert ERIS supervise et contribue à la mise en place de l'infrastructure, assurant la qualité, le respect des délais et des coûts.</i></p> <p><i>Il s'assure que les infrastructures sont déployées selon les spécifications, en utilisant des méthodes de gestion de projet (Cycle en V, Agilité), s'aidant d'outils tels que JIRA ou</i></p>	<p>C15 - Contribuer à la mise en place, au contrôle et à l'administration de l'infrastructure, en mobilisant ses compétences techniques, en collaborant avec les équipes pluridisciplinaires et en documentant la solution pour déployer les éléments techniques de la solution.</p>		<p>Cr15.1 - Les éléments techniques mis en place respectent la topologie.</p> <p>Cr15.2 - La documentation produite permet à une tierce personne de prendre connaissance des détails de l'implémentation et/ou de la reproduire à l'identique.</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p><i>Microsoft Project pour suivre l'avancement et gérer les équipes techniques.</i></p> <p><i>Il collabore étroitement avec les équipes de développement et d'exploitation pour coordonner les activités et résoudre les problèmes techniques. Il met en place des processus de validation et de tests pour s'assurer que les solutions déployées répondent aux attentes.</i></p> <p><i>Il met en place l'automatisation des processus d'intégration, de déploiement et de maintenance des systèmes et applications dans un mode de fonctionnement DevOps. Il utilise des outils tels que Ansible, Jenkins, AWS, GitLab CI, et Azure DevOps.</i></p>	<p>C16 - Automatiser les processus d'intégration, de déploiement et de maintenance des systèmes et applications en utilisant des outils d'orchestration, de gestion de déploiement et de DevOps et en contrôlant le résultat par l'analyse des logs produits pour assurer la fiabilité et la reproductibilité des mises en production.</p>		<p>Cr15.3 - Les contrôles sont effectués avec rigueur et permettent de garantir l'adéquation de l'équipement mis en place avec les exigences de fonctionnement et de performance.</p> <p>Cr16.1 - Les outils sélectionnés et configurés permettent l'automatisation de l'intégration, le déploiement et la maintenance des systèmes et applications.</p> <p>Cr16.2 - Les mises en production satisfont les critères de fiabilité et de reproductibilité.</p> <p>Cr16.3 - Les contrôles opérés permettent d'assurer la traçabilité des mises en production et attester de leur succès.</p>
<p>A2.3 - Gestion des incidents et des tickets</p> <p><i>L'expert ERIS organise et supervise la gestion des incidents pour assurer une résolution rapide et efficace des problèmes techniques. Il utilise des systèmes de gestion des tickets (ITSM) comme ServiceNow ou JIRA Service Desk pour suivre, prioriser et résoudre les incidents.</i></p> <p><i>L'expert ERIS définit des processus standardisés pour la création, l'attribution, le suivi des tickets et leur élévation (support N1/N2/N3),</i></p>	<p>C17 - Organiser et piloter la gestion des incidents et du support en définissant les processus standardisés pour la création, l'attribution, le suivi des tickets et leur élévation, dans un cadre d'amélioration continue et en s'appuyant sur des outils de gestion des tickets (ITSM), pour suivre, prioriser et résoudre les incidents, ainsi qu'assurer une résolution rapide et efficace des problèmes techniques.</p>	<p>Evaluation n°3 : mise en situation professionnelle – étude de cas sur l'organisation de la gestion des incidents et du support Epreuve écrite individuelle</p>	<p>Cr17.1 - La gestion des incidents et du support est organisée autour d'une solution de gestion de tickets permettant leur priorisation, attribution, suivi et éventuelle élévation.</p> <p>Cr17.2 - L'organisation choisie permet de respecter les délais de prise en charge fixés dans les SLA.</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p><i>assurant une communication claire entre les équipes techniques et les utilisateurs finaux.</i></p> <p><i>Dans le cadre de l'amélioration continue des services, il analyse les incidents récurrents pour identifier les causes profondes et mettre en place des mesures préventives.</i></p> <p><i>Il assure le pilotage opérationnel de l'équipe en charge de la gestion des incidents et assure le support N3 (expert).</i></p>			<p>Cr17.3 - La solution retenue, la structuration du support en niveaux, et les processus mis en œuvre permettent une gestion efficace des incidents et la capitalisation des réponses mises au point.</p> <p>Cr17.4 - L'organisation du support facilite la détection des incidents récurrents et la mise en place de mesures préventives.</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p>A3 – Pilotage de la Sécurité des Systèmes d'Information</p> <p>A3.1 - Elaboration d'une politique de sécurité des SI</p> <p><i>L'expert ERIS participe à l'élaboration et la mise en œuvre de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'entreprise, en conformité avec les standards ISO 2700x, le RGPD et les recommandations de l'ANSSI. Il travaille en collaboration avec le Responsable de la Sécurité des Systèmes d'Information (RSSI).</i></p> <p><i>Il mène une veille active sur la cybersécurité (nouvelles menaces, vulnérabilité, disponibilité des correctifs) tant en français qu'en anglais technique.</i></p> <p><i>Il définit des procédures de réponse aux incidents pour protéger les données et les systèmes de l'entreprise.</i></p> <p><i>L'expert ERIS décide de politiques de gestion des accès et des identités (IAM) à travers des outils de sécurité tels que le MFA, SSO...</i></p> <p><i>En collaboration avec le RSSI, il assure l'amélioration continue de la sécurité en veillant à ce que la PSSI soit régulièrement mise à jour pour faire face aux nouvelles menaces et évolutions réglementaires. Il met en place des audits de sécurité réguliers.</i></p>	<p>C18 - Conduire une veille active en matière de cybersécurité, en analysant régulièrement les bulletins de sécurité, les publications des organismes de référence tant francophones qu'anglophones et en partageant les fruits de ses recherches conformément aux us de l'équipe (rapport/article, réseau social interne, plateforme collaborative), afin d'anticiper les menaces et vulnérabilités émergentes et mener des actions correctives.</p> <p>C19 - Participer à l'élaboration et à la mise en œuvre de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'entreprise, en s'appuyant sur les standards, en s'appuyant sur une analyse des risques de sécurité, en définissant des mesures, rôles, responsabilités, procédures et protocoles, en collaboration avec le Responsable de la Sécurité des Systèmes d'Information (RSSI) pour protéger les données et les systèmes de l'entreprise.</p>	<p>Evaluation n°4 : rapport de veille sur la cybersécurité en anglais Epreuve écrite individuelle (Compétence C18)</p> <p>Evaluation n°5 : mise en situation professionnelle simulée – rédaction d'une politique de sécurité Epreuve écrite individuelle (Compétences de C19 à C21)</p>	<p>Cr18.1 - Le rapport de veille est rédigé en anglais technique. La qualité de la rédaction permet la compréhension pour un collaborateur anglophone.</p> <p>Cr18.2 - Le contenu du rapport de veille identifie clairement les sources, les confronte et permet d'adapter des actions correctives.</p> <p>Cr19.1 - L'analyse des risques de sécurité est actualisée, à la fois au niveau des menaces, mais aussi pour intégrer les évolutions de l'infrastructure. Elle permet de prioriser les évolutions à apporter à la PSSI.</p> <p>Cr19.2 - Les dispositions prises pour faire évoluer la PSSI prennent en compte les risques, les recommandations de l'ANSSI et les moyens mobilisables pour la mise en œuvre.</p> <p>Cr19.3 - Les dispositions prises sont conformes avec les standards et réglementations en vigueur (ISO 2700x, RGPD).</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
	C20 - Auditer la sécurité en collaboration avec le Responsable de la Sécurité des Systèmes d'Information (RSSI) en couvrant les volets organisationnels, physiques et techniques afin de vérifier la mise en œuvre de la politique de sécurité et assurer son amélioration continue.		Cr20.1 - L'audit couvre de façon méthodique les volets physiques, techniques et organisationnels de la politique de sécurité et s'appuie sur une méthodologie d'audit existante (telle que ISO 27001). Cr20.2 - Les résultats de l'audit sont consignés dans un rapport permettant de conclure quant à la conformité de la mise en œuvre de la politique de sécurité et l'atteinte de ses objectifs. Des axes d'améliorations sont mis en avant le cas échéant.
A3.2 - Formation et Sensibilisation à la Cybersécurité <i>L'expert ERIS forme le personnel aux bonnes pratiques de sécurité informatique et développe des programmes de sensibilisation au moyen d'ateliers, d'exercices de simulation d'attaque, et de campagnes de phishing.</i>	C21 - Sensibiliser le personnel aux bonnes pratiques de la sécurité informatique en conformité avec les préconisations de l'ANSSI au moyen d'ateliers, de documentation, d'exercices de simulation d'attaque, et de campagnes de phishing afin de diminuer les comportements à risques et de contribuer à l'amélioration continue de la sécurité de l'entreprise.		Cr21.1 - Les actions de sensibilisation proposées diffusent et vulgarisent la PSSI et sont adaptées au public concerné (format, durée, fréquence). Cr21.2 - L'ensemble des actions proposées suit une démarche d'amélioration continue afin de pouvoir en évaluer la pertinence et l'efficacité.
A3.3 - Evaluation de la sécurité : Ethical Hacking et tests de pénétration <i>L'expert ERIS réalise des tests de pénétration pour identifier et corriger les vulnérabilités. Il utilise des outils tels que Metasploit, OpenVAS et Nessus pour simuler des attaques et évaluer la robustesse des infrastructures.</i>	C22 - Eprouver la sécurité de l'infrastructure sous la responsabilité du RSSI, au moyen de tests de pénétration, de simulations d'attaques, d'outils d'analyse de sécurité afin d'évaluer la robustesse des systèmes et la réactivité des équipes.	Evaluation n°6 : mise en situation professionnelle – Etude de cas écrite sur la base d'un rapport d'audit Epreuve écrite individuelle (Compétences C21 à C23)	Cr22.1 - Les tests permettent à la fois d'évaluer la robustesse des systèmes et la réactivité des équipes.

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p><i>Il consigne les vulnérabilités découvertes et décide de l'application des mesures correctives en collaboration avec les équipes techniques.</i></p> <p><i>Il organise des simulations d'attaques pour tester la réactivité des équipes et la robustesse des systèmes.</i></p>			<p>Cr22.2 - Les observations faites suite aux tests sont prioritaires et permettent d'améliorer l'application de la PSSI ou des dispositifs de sécurité.</p>
<p>A3.4 - Investigation et Analyse des Incidents de Sécurité : Analyse Forensic*</p> <p><i>L'expert ERIS effectue des analyses forensic pour enquêter et répondre aux incidents de sécurité.</i></p> <p><i>Il examine les systèmes compromis, retrace les actions malveillantes, et collecte des preuves numériques.</i></p> <p><i>Il prépare des rapports d'investigation détaillés pour les audits de sécurité.</i></p> <p><i>Il met en place des protocoles de conservation de preuves pour garantir leur intégrité et leur admissibilité en justice, conformément aux recommandations de l'ANSSI.</i></p>	<p>C23 - Investiguer et analyser les incidents de sécurité, en conformité avec les recommandations de l'ANSSI, en examinant les systèmes compromis, en retraçant les actions malveillantes, et en collectant les preuves numériques afin de préparer des rapports en vue des audits de sécurité et conserver des preuves légales.</p>		<p>Cr23.1 - Les investigations se font dans le respect du cadre légal, et suivent une démarche conforme avec les réglementations de l'ANSSI et veillent à ne pas détruire de preuves.</p> <p>Cr23.2 - L'analyse méthodique des systèmes compromis permet de retracer les actions malveillantes et de collecter des preuves. Les preuves sont consignées dans un rapport d'analyse.</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p>A3.5 - Supervision et Gestion des Centres Opérationnels de Sécurité (SOC)</p> <p><i>L'expert ERIS intervient dans les centres opérationnels de sécurité (SOC), surveillant les alertes de sécurité en temps réel et gérant les incidents de sécurité.</i></p> <p><i>Il utilise des solutions SIEM telles que Splunk et ELK, et des outils EDR/xDR pour collecter et analyser les données de sécurité, détecter les anomalies et orchestrer des réponses rapides et efficaces aux incidents.</i></p> <p><i>Il automatise le déploiement des correctifs en utilisant des outils tels que les playbooks et assure une surveillance continue pour maintenir la sécurité de l'infrastructure.</i></p> <p><i>Il veille à la mise en place de procédures de réponse aux incidents bien définies et régulièrement testées, en accord avec les standards de l'ANSSI.</i></p>	<p>C24 - Contribuer au fonctionnement du Centre Opérationnel de Sécurité (SOC), en gérant les incidents de sécurité au moyen de solutions SIEM, en analysant les données de sécurité, en détectant les anomalies, en orchestrant des réponses rapides et efficaces, en pilotant le déploiement des correctifs, s'il y a lieu de façon automatisée, et en assurant une surveillance continue afin de maintenir la sécurité et la résilience de l'infrastructure.</p>		<p>Cr24.1 - La détection d'incidents de sécurité par l'analyse des données de sécurité et recherche d'anomalies est effective.</p> <p>Cr24.2 - Les alertes et contre-mesures déclenchées suite à la détection d'un incident de sécurité permettent la sécurisation du SI.</p> <p>Cr24.3 - La diffusion de correctifs de sécurité de façon automatisée ou non est opérationnelle.</p> <p>Cr24.4 - L'analyse post-incident permet de retracer sa chronologie et d'apporter les corrections nécessaires au niveau de la PSSI.</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p>A4 – Pilotage de Projets et Conduite du Changement</p> <p>A4.1 - Pilotage de projets</p> <p><i>L'expert ERIS pilote des projets en utilisant une méthodologie adaptée au contexte (agilité comme Scrum et Kanban, cascade, cycle en V) et en supervisant des équipes pluridisciplinaires.</i></p> <p><i>Il participe à la prise de décision quant au traitement interne ou externe du projet et assure le cas échéant la sélection et le suivi de la prestation.</i></p> <p><i>Il utilise des outils de gestion de projet adaptés à la méthodologie retenue pour planifier, exécuter et suivre les projets (tel que Excel, JIRA, Microsoft Project).</i></p> <p><i>Il s'assure que les projets respectent les délais, les budgets (estimation et contrôle des coûts, et suivi budgétaire) ainsi que les exigences de qualité en matière de livrables.</i></p> <p><i>Il anime des réunions de suivi et de coordination pour s'assurer que toutes les parties prenantes sont alignées et informées de l'avancement des projets.</i></p>	<p>C25 - Piloter un projet au moyen d'une méthode de gestion de projet et des outils adaptés au contexte, en analysant le besoin, en rédigeant les documents d'initialisation et de suivi de projet adaptés à la méthode, en mobilisant les ressources et moyens nécessaires, pour gérer les équipes, s'assurer que les solutions déployées répondent aux attentes de l'entreprise et garantir la qualité des livrables, le respect des délais et des coûts.</p> <p>C26 - Assurer le suivi et le reporting du projet en s'adaptant aux parties prenantes concernées (COPIIL, équipe projet, client) afin de garantir une communication claire, efficace et adaptée aux besoins, de faciliter la prise de décision, d'assurer la transparence sur l'avancement du projet, et de maintenir l'alignement des objectifs.</p>	<p>Evaluation 7 : Mise en situation reconstituée</p> <p>Etude de cas portant sur un scénario de la mutation d'une entreprise sur la base d'un important changement IT.</p> <p>Ecrit et oral</p> <p>(Compétences de C25 à C29)</p>	<p>Cr25.1 - L'analyse des besoins est précise et fidèle à la demande et permet d'organiser le projet et arbitrer son traitement interne ou externe.</p> <p>Cr25.2 - La méthode de gestion de projet et outils retenus permettent un suivi efficace et adapté au projet.</p> <p>Cr25.3 - Les documents d'initialisation et de suivi permettent de cadrer le projet de façon efficace.</p> <p>Cr25.4 - Les ressources et moyens mobilisés (internes ou externes) sont adaptés aux objectifs en termes de qualité, de délais et de coûts de façon optimisée.</p> <p>Cr26.1 - Le reporting est adapté dans son format (rapport/présentation), dans sa mise en forme visuelle et son contenu au public auquel il est destiné.</p> <p>Cr26.2 - La description de l'avancement du projet offre une vision claire et détaillée, et permet, le cas échéant, de prendre une décision éclairée.</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<p>4.2 - Gestion du Changement et de la Transformation IT</p> <p><i>L'expert ERIS élabore et met en œuvre des plans de conduite du changement en s'appuyant sur des référentiels comme ITIL.</i></p> <p><i>Il pilote la mise en production des systèmes et applications, évaluant les risques et les impacts, et développant des stratégies pour les atténuer. Il informe les parties prenantes contribuant ou étant impactées par la mise en production.</i></p> <p><i>Il organise la formation des utilisateurs pour faciliter l'acceptation et l'appropriation des nouveaux outils et processus.</i></p>	<p>C27 - Elaborer et mettre en œuvre la conduite du changement en s'appuyant sur des référentiels tels qu'ITIL, en réalisant une analyse de risques, en mettant au point une procédure de mise en production et au moyen de documentations et/ou de formations pour les utilisateurs concernés (acteurs comme usagers), afin de minimiser l'impact d'une évolution (mineure, delta ou majeure) de l'infrastructure sur l'environnement de production.</p>		<p>Cr27.1 - L'analyse de l'existant, des impacts du changement et des risques afférents permet de formaliser un plan de conduite du changement structuré.</p> <p>Cr27.2 - L'accompagnement des parties prenantes est pris en compte au travers de documentation et/ou d'actions de formation favorisant l'adaptation.</p>
<p>4.3 – Accompagnement et Développement des équipes projets</p> <p><i>L'expert ERIS identifie les besoins en compétences, développe les talents et planifie la formation des collaborateurs.</i></p> <p><i>Il contribue au recrutement des collaborateurs en assurant la caution technique.</i></p> <p><i>Il participe à l'évaluation de la performance des collaborateurs en mesurant l'écart entre les objectifs et le réalisé. Il organise des feedbacks réguliers pour contribuer à l'amélioration continue.</i></p>	<p>C28 - Développer la performance de l'équipe en identifiant les besoins en compétences, en développant les talents, en planifiant la formation des collaborateurs, en participant à leur évaluation, et en mesurant l'écart entre les objectifs et le réalisé, pour améliorer la réussite des projets dans le respect des exigences fixées.</p>		<p>Cr28.1 - Le plan de formation est motivé par la démonstration de l'inadéquation entre des capacités actuelles de l'équipe et les besoins en compétences des projets actuels et futurs.</p> <p>Cr28.2 - Les actions de remédiation du dans le plan de formation identifient des temps, des moyens et des objectifs mesurables permettant d'attester de leur efficacité.</p>

RÉFÉRENTIEL D'ACTIVITÉS <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	RÉFÉRENTIEL DE COMPÉTENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
	<p>C29 - Contribuer au recrutement des collaborateurs en participant aux rédactions de fiches de poste, en assurant une caution technique au moyen d'évaluations des compétences lors des entretiens, et en mettant l'accent sur l'inclusion notamment des personnes en situation de handicap, afin de contribuer à la construction d'une équipe diversifiée, reflétant les valeurs de l'égalité des chances et de la responsabilité sociétale (RSE).</p>		<p>Cr29.1 - Les missions qui figurent sur la fiche de poste correspondent aux savoir-faire et savoirs-être du poste à pourvoir.</p> <p>Cr29.2 - La fiche de poste et les modalités prévues sont respectueuses des valeurs d'égalité des chances et de la responsabilité sociétale.</p> <p>Cr29.3 - Les modalités d'évaluation prévues (questions à l'oral, tests écrits ou techniques) permettent de positionner les candidats et sont adaptables en cas de situation de handicap.</p>

La certification d'Expert Réseaux Infrastructures et Sécurité est attribuée après validation des 4 blocs de compétences et de l'évaluation complémentaire représentée par le Projet d'Étude Professionnel.