ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

5 - REFERENTIELS

Article L6113-1 En savoir plus sur cet article... 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.* »

Bloc n°1 –Identifier les solutions techniques de sécurité d'un SI face à la menace			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A1.1. Protection des composants physiques d'un système d'information - **T1 : Identification des 5 composants d'un ordinateur** - **T2 : proposition de solutions pour renforcer la sécurité des composants d'un ordinateur**	• **C1** Renforcer la sécurité des 5 composants d'un ordinateur (matériel, représentation et stockage de données, manipulation des données et logique, fichiers et enregistrements, Cloud Computing), en vue de protéger le système matériel, par une analyse de leur périmètre et de leur rôle, ainsi que des risques associés.	E1 Etude de cas Renforcer la sécurité technique d'un SI Une étude de cas sert de fil rouge pour le bloc n°1 : Renforcer la sécurité technique d'un SI. Il s'agit de l'étude de cas : Lessons Learned from NSA Storing Vulnerable data. A partir de la distribution du cas pratique, les candidats ont 4 heures pour présenter un compte rendu écrit, sous forme de présentation Powerpoint, devant un jury (Durée 30 mn). La présentation doit comprendre :	C1 Les 5 composants sont listés et présentés. C1 Les différentes caractéristiques sont expliquées. C1 Les risques associés sont déterminés. C1 Des solutions sont proposées pour renforcer la sécurité de chacun des composants d'un ordinateur.
A1.2. Protection des composants logiques d'un système d'information • **T3 : Identification des éléments clés d'un système d'information que**	• **C2** Renforcer la sécurité des systèmes d'exploitation, la terminologie et les fonctions de la virtualisation et des containers, en vue de protéger la sécurité des composants logiques d'un système d'information, par une analyse de leur périmètre et de leur rôle, ainsi que des risques associés		C2 : Une plate-forme virtuelle (dans le cadre d'un projet de cloud Computing) est montée. Cette plate-forme est paramétrée et optimisée pour renforcer la sécurité de l'information.

sont le système d'exploitation, la virtualisation et les containers • **T4 Proposition de solutions pour renforcer la sécurité des 3 composants logiques**		- L'identification des composants techniques, logiques & réseaux, les données ainsi que les systèmes embarqués - les mesures de sécurité techniques à mettre en place pour renforcer la sécurité technique du système Une partie des réponses se trouve sur les sites de veille en cyber sécurité afin d'inciter les candidats à mettre à jour en continu leur connaissances.	
A1.3. Protection des réseaux • **T6 : description du modèle OSI des 7 couches du réseau et protection de chacune de couches. Application aux réseaux TCP/IP.**	• C3 Renforcer la sécurité des 7 couches du modèle OSI de description des réseaux, en déterminant les risques associés à chacune des couches, par la reconnaissance des différents types d'attaque sur chacune des couches du modèle OSI • C4 Appliquer aux réseaux TCP/IP les principes de la démarche de protection des 7 couches du modèle OSI		C 3 : Les attaques sur les différentes couches du modèle OSI de description des réseaux sont repérées : identification des différents composants d'un réseau (matériel et logiciel), les paquets, les types de réseau, les adresses, les protocole TCP & UDP, les sous-réseaux, les protocoles de messagerie (SMTP…) les DNS, les forward et reverse look up, les protocoles ICMP / DHCP, etc. C4 : les attaques sur les différentes couches du modèle TCP/IP sont passées en revue, identifiées, et corrigées
A1.4. Protection des données personnelles et des informations • **T8 : Identification des données personnelles selon les critères du RGPD et d'ISO 27701** • **T9 : application des mesures de sécurité techniques pour protéger les données d'identification personnelles**	• C5 Cartographier les données personnelles déterminer leur criticité et leur valeur selon les exigences du RGPD et d'ISO 27701 • C6 Appliquer à la sécurité des données les mesures techniques de protection adéquates en fonction de leur valeur : chiffrement symétrique et asymétrique, anonymisation, pseudonymisation		C5 Une cartographie des données est réalisée pour identifier leur localisation, leur criticité et leur valeur C6 : les mesures de protection adéquates sont appliquées pour protéger au mieux les données en fonction de leur valeur et de leur usage
A1.5 Protection des systèmes embarqués • **T10 : identification des systèmes embarqués** • **T11 : application des mesures de protection techniques pour renforcer leur sécurité**	• C7 Identifier les systèmes embarqués, les PLC (Programmable Logic Controller) et les RTU (Remote Terminal Unit), identifier les protocoles sous-jacents : (comme Modbus) et les systèmes Scada de supervision, pour déterminer leurs vulnérabilités et appliquer les mesures de sécurité techniques pour renforcer la sécurité des systèmes embarqués		C7 Une cartographie des systèmes embarqués est réalisée C7 Une analyse des vulnérabilités est réalisée C7 Des mesures de renforcement de la sécurité sont proposées

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

A1.6 La veille en cybersécurité • **T12 Mise en place un processus de veille en cybersécurité**	• C8 Suivre les flux d'information en cybersécurité pour être informé des dernières menaces et des solutions à déployer par la mise en place d'un système de veille en cyber sécurité		C8 Un processus de veille en cybersécurité est proposé C8 Un système de traitement des informations est proposé pour identifier les informations les plus pertinentes en priorité

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

Bloc n°2 – Opérer et surveiller les mesures de sécurité d'un SI			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A1.1 Gestion des événements et les incidents de sécurité de l'information • **T1 Conception d'un processus de gestion des événements et des incidents de sécurité de l'information** • **T2 Identification des pistes d'automatisation et d'outillage concernant l'identification, la gestion des priorités et le traitement des événements et des incidents de cyber sécurité**	• C1 Déployer un système de monitoring de l'activité en sécurité de l'information pour repérer les événements et les incidents de sécurité, afin de les traiter • C2 Concevoir un processus et un flux de traitement des événements et des incidents en s'appuyant sur la norme ISO 27035, pour automatiser le traitement des événements et des incidents	E1 : Cas pratique Suite à une série d'incidents de sécurité significatifs, une entreprise décide dans un premier temps de réaliser une enquête technico légale pour comprendre l'origine des incidents, puis de réaliser un pen test pour tester la vulnérabilité du système d'information, et afin d'automatiser le monitoring et le traitement des incidents de sécurité A partir de la distribution du cas pratique, les candidats ont 4 heures pour présenter un compte rendu écrit, sous forme de présentation Powerpoint, devant un jury (Durée 30 mn). La présentation doit comprendre : - Le résultat de l'analyse forensic sur l'origine des incidents de cyber sécurité - Le résultat du pen test et les suggestions	C1 Face à une série d'événements, les incidents de sécurité sont distingués des faux positifs C2 les incidents sont classés par ordre de priorité et assignés aux bons groupes de supports
A.1.2 Réalisation d'une enquête technico légale (Forensic) • **T3 identification de l'origine d'une série d'incidents de cyber sécurité par l'application des techniques de Forensic**	• C3 mener une enquête technico légale (Forensic) en s'appuyant sur la norme ISO27037, afin d'identifier la cause des incidents de cyber sécurité et d'y apporter des solutions		C3 Des preuves numériques d'intrusion dans un système d'information sont identifiées, collectées, acquises et préservées selon les recommandations de la norme ISO 27037
A1.3 Réalisation d'un test d'intrusion • **T4 : réaliser un pen test (test d'intrusion) pour tester les vulnérabilités d'un système d'information et renforcer la sécurité de celui-ci**	• C4 réaliser un pen test selon les standards du marché (planification, reconnaissance, test de vulnérabilité, exploitation, effacement des traces, rapport) pour identifier les vulnérabilités d'un système d'information et ainsi renforcer sa sécurité		C4 un test d'intrusion est mené de bout en bout

		d'amélioration de la sécurité du système d'information - Les processus de gestion des incidents de sécurité	

Bloc n°3 – Auditer la maturité de la cybersécurité d'un système d'information			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A3.1. Mise en place un système de management de la sécurité de l'information (SMSI) - **T1** : Mise en place de la planification, le déploiement, le contrôle et l'amélioration d'un SMSI selon la norme ISO 2700A de sécurité de l'information - **T2** : évaluation de la maturité du SMSI - T3 Proposition de pistes d'amélioration pour renforcer la maturité d'un SMSI	• C1 Déployer un SMSI pour apporter un cadre de gouvernance et de gestion de la sécurité d'un système d'information en s'appuyant sur les meilleures pratiques d'ISO • C2 évaluer la maturité du SMSI pour renforcer la sécurité du système d'information en s'appuyant sur la norme ISO 15504	E2 : Etude de cas Auditer la sécurité organisationnelle d'une entreprise et déployer une démarche de gouvernance de la sécurité L'étude de cas porte sur une organisation qui a subi une fuite de données. Celle-ci évalue la maturité de la sécurité de son système d'information en s'appuyant d'une part sur : - Le système de management de la sécurité de l'information (ISO 27001) - D'autre part sur les 114 mesures de sécurité proposées par ISO 27001 et décrites dans ISO 27002, et leur niveau de maturité Le candidat a 4 heures pour présenter un compte rendu écrit, sous forme de présentation Powerpoint, devant un jury (Durée 30 mn).	C1 Un plan d'amélioration continue de la politique de sécurité SI est proposé C2 Une analyse de la maturité du SMSI existant est réalisée
A3.2 Analyse de risque - **T4 analyse des risques en sécurité de l'information selon les meilleurs pratiques d'ISO 27005 et Ebios**	• C3 Réaliser une analyse de risque pour identifier les vulnérabilités et menaces potentielles en sécurité du système d'information et s'appuyant sur ISO 27005 et Ebios • C4 Proposer des mesures de traitement pour renforcer la sécurité du système d'information en s'appuyant sur l'analyse de risques, ainsi que les meilleures pratiques de l'OWASP, du MITRE		C3 Une analyse de risque est réalisée, selon les meilleures pratiques d'ISO 27005 et Ebios C4 Un plan de mesure de traitement est proposé selon les meilleures pratiques de l'OWASP et du MITRE
A3.3 Audit de maturité des mesures de sécurité déployées par l'organisation	• C5 Analyser l'efficacité et l'efficience des mesures de sécurité mises en place par l'organisation, pour identifier les plus faibles et les moins pertinentes,		C5Une déclaration du domaine d'applicabilité (la liste des mesures à

- **T4 : revue et évaluation des mesures de sécurité proposées par ISO 27001 (et décrites dans ISO 27002)**	afin de renforcer la sécurité du système d'information	La présentation doit comprendre : - L'analyse des risques en sécurité du système d'information - Un compte rendu d'audit de maturité sur le SMSI ainsi que les mesures de sécurité - Le degré de conformité réglementaire et juridique de l'organisation. - Proposition de pistes d'amélioration pour renforcer la sécurité du système d'information	mettre en place) et une matrice de traçabilité de leur état sont fournies.
A3.4. Conception d'une roadmap d'amélioration de la sécurité du système d'information - **T5** : planification d'un projet de mise en place de l'ensemble des mesures de sécurité nouvelles ou à renforcer, suite à l'audit de maturité	• C6 préparer un plan de projet comprenant l'ensemble des mesures de sécurité manquantes ou à renforcer, sur à l'audit de maturité, pour renforcer la sécurité du système d'information		**C6 :** un plan de projet (calendrier, ressources, livrables, coûts, délais, risques) est proposé pour l'ensemble des mesures de sécurité manquantes ou à renforcer

Bloc n°4 – Piloter un projet et communiquer en cybersécurité

RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A4.1. Réalisation d'un business case et d'un plan de gestion de projet de sécurisation de l'information - **T1 :** Conception d'un projet de cyber sécurité - **T2 :** Adaptation aux changements de contexte organisationnel, technique et légal	• **C1** Concevoir un projet de cyber sécurité, afin de planifier les différentes activités à réaliser, par l'application d'une méthode de gestion de projet • **C2** Piloter le plan de gestion de projet, afin de l'adapter aux évolutions, par l'application de processus de gestion des changements, de monitoring et de reporting	E4 jeu de rôle et de simulation Après lecture et analyse des informations disponibles dans le sujet, les candidats travaillent par groupe et présentent devant un jury le résultat de leurs analyses. Les candidats ont 4 heures pour présenter un compte rendu écrit, sous forme de présentation Powerpoint, devant un jury (Durée 30 mn). La présentation doit comprendre : Au sein d'une équipe projet, les candidats doivent gérer plusieurs situations : - La direction générale de l'équipe Clients exige un business Case pour valider un projet de déploiement de la certification ISO 27001, - Les candidats doivent gérer plusieurs conflits : grève des équipes car la crainte pour leurs emploi, gestion d'une situation de crise et	C1 : un business est restitué et présenté C2 : le plan de projet est restitué et présenté (ressources, gestion du calendrier, présentation des indicateurs de suivi, budget)
A4.2. Pilotage du changement • **T3 :** gestion de la conduite du changement et de la résistance au changement	• **C3** Piloter une démarche de conduite du changement, en vue d'optimiser la démarche de sécurité de l'information et de lever les freins humains, par l'application d'une méthode de type Kotter et les modèles de communication de type PCM, PNL et analyse transactionnelle		C3 : une démarche de conduite du changement est présentée et restituée C3 : des entretiens de simulation sont menés, en utilisant des techniques de communication de type PCM, PNL et analyse transactionnelle, pour gérer les craintes des parties prenantes lors d'une démarche de changement organisationnel
A4.2. Communication d'une démarche de cybersécurité • **T4 :** développement et maintien d'une culture de la sécurité de l'information	• **C4 C**ommuniquer avec la direction générale et le conseil d'administration, afin de les impliquer dans la démarche de sécurité de l'information, par la compréhension de leurs enjeux et la présentation de rapports en sécurité de l'information adaptés à leurs fonctions		C4 : une chaîne de la valeur et un Business Model Canvas sont présentés, pour comprendre la mission, ainsi que la stratégie de l'entreprise C4 : un rapport de sécurité de l'information est présenté à une

	• **C5** aligner la culture de cyber sécurité sur la stratégie de l'entreprise, afin de concevoir la meilleure feuille de route, par l'utilisation des frameworks et outils les plus appropriés et pertinents	conduite du changement. - Proposition d'un plan de sensibilisation de l'ensemble du personnel car les nouveaux usages du Cloud Computing exige des comportements adéquats en termes de protection et d'accès à des informations critiques, externalisés chez un fournisseur tiers. - Proposition d'un plan de communication de crise si une fuite de données est révélée	direction générale ou fonctionnelle lors d'une revue de direction C5 : une feuille de route est rédigée et contient les outils appropriés au projet
A4.4. Mangement d'équipe • **T5 :** Direction l'équipe	• **C6** Motiver les équipes, afin d'atteindre les objectifs de sécurité de l'information, par l'acquisition de connaissances et de compétences en leadership (la construction d'un climat de confiance, la création et la construction d'équipes, le leader comme facilitateur de projets, le coaching et le sponsorship, le challenging conversation) • **C7** Gérer les conflits afin de renforcer le climat de confiance des équipes et d'optimiser les talents, par l'application de techniques de leadership (l'écoute active, le feed-back, apprendre à déléguer, le mentoring) • **C8** Accompagner une personne en situation de handicap afin de faciliter son intégration dans l'équipe et dans son environnement de travail		C6 : L'écoute active, La reformulation et La maïeutique sont utilisées lors des entretiens de simulation Une analyse est restituée en modélisant la complexité de la situation organisationnelle C7 Le feed back, la délégation et le mentoring sont utilisés lors d'un deuxième entretien de simulation C8 Une proposition spécifique est formulée pour faciliter la prise en compte d'une personne en situation de handicap dans un contexte de crise
A.4.5 Communication de crise	• **C9** Créer un plan d'actions pour le déploiement et la gestion des outils de communication digitaux en s'appuyant sur ISO 22301 • **C10** Créer le contenu de communication accessible au grand public en concertation avec les professionnels concernés et en préservant l'e-reputation en s'appuyant sur ISO 22361 (Crisis & resilience)		C9 Un plan de communication interne de crise est présenté pour gérer la révélation d'une fuite de données personnelles des clients de l'organisation C10 Un plan de communication externe est présenté selon les critères de la norme ISO22361

Bloc de spécialisation n°1 – Concevoir et déployer un système d'information sécurisé avec une approche DevSecOps

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A3.1. Projet de Transformation numérique - **T1** : la fonction d'architecte dans la transformation numérique de l'entreprise - **T2** : cartographie, conception, modélisation et simulation d'un système d'information sécurisé	• **C1** Faire évoluer le système d'information afin de répondre aux attentes du métier en termes de sécurité, par une démarche de cartographie et d'urbanisation du système d'information • **C2** Concevoir une roadmap de transformation dans l'entreprise afin de répondre aux exigences de sécurité de l'information, par l'application des méthodes de modélisation et de simulation	E3 Etude de cas Concevoir un système d'information sécurisé L'étude de cas porte sur une organisation qui décide de migrer l'ensemble de son système d'information vers une solution externalisée de cloud computing. A partir de la distribution, les candidats ont 4 heures pour présenter un compte rendu écrit, sous forme de présentation Powerpoint, devant un jury (Durée 30 mn). La présentation doit comprendre : - Les enjeux et motivations d'une transformation numérique pour l'organisation, le rôle et l'implication de la direction générale ; - Le dossier d'architecture matériel, logiciel, base de données et réseau. - Un plan de projet de développement	**C1 :** Une démarche d'urbanisation à l'aide d'outils de modélisation des processus métier et des systèmes d'information, est présentée. **C2 :** une roadmap de transformation est présentée, en vue de faire évoluer le système d'information par rapport aux exigences du métier et des nouvelles règles de sécurisation des données (notamment des données personnelles)
A3.2. Architecture hardware - **T3** : les meilleures pratiques de l'architecture technique à intégrer dans un dossier d'architecture et à déployer dans un environnement de production	• **C3** Concevoir et déployer une architecture technique sécurisée, afin de renforcer la sécurité lors de la conception et la maintenance des composants d'un système d'information (réseau/télécom, stockage des informations, hardware, système d'exploitation, virtualisation, Cloud et containers), par l'application des meilleures pratiques dans ce domaine • **C4** Appliquer un référentiel comme Devops, afin de pouvoir immédiatement travailler avec les professionnels du marché, par l'application de cette méthodologie à une étude de cas		**C3 :** une démarche de conception d'une architecture technique est présentée C4 la démarche de conception est bâtie sur une approche du référentiel DevOps
A3.3. Architecture logicielle - **T4** : les meilleures pratiques de l'architecture technique à intégrer dans un dossier d'architecture et à	• C5 Concevoir et déployer une architecture logicielle sécurisée, afin de renforcer la sécurité lors de la conception et la maintenance des composants d'une application et de ses composants (architecture n-tiers, Java et .Net, cycle de développement sécurisé,		**C5 :** une démarche d'analyse de la sécurité d'une application est présentée, ainsi que des propositions de mesures de sécurité pour combler ses failles

déployer dans un environnement de production	architecture réactive et Cloud native, intégration des API, architecture client serveur/Web et mobile, architecture de données avancée, pipeline, gestion des tests), par l'apprentissage et l'application des meilleures pratiques dans ce domaine	sécurisé pour les scripts d'automatisation et de paramétrage de la migration des données, dans un environnement de type PaaS (Platform As A Service) - Une revue de code sécurisée en appliquant les meilleures pratiques de Dev Sec Ops	
A3.4. La gestion d'un projet de développement sécurisé - **T5** : Les meilleurs pratiques du développement sécurisé en s'appuyant sur Dev Sec Ops	• C6 Gérer un projet de développement sécurisé pour minimiser attaques sur les logiciels en fonctionnement afin de garantir la sécurité des programmes et des systèmes d'information • C7 Appliquer les meilleures pratiques de Dev Sec Ops par des cycles de développement rapides et fréquents en intégrant la sécurité du code dès la conception des applications		**C6 :** un plan de projet de développement sécurisé est présenté, intégrant les meilleures pratiques de Dev Sec Ops C7 : une revue de code est présentée, corrigeant les vulnérabilités d'un logiciel liée à une programmation non sécurisée

Bloc de spécialisation n°2 – Préparer un audit de certification en sécurité et continuité de l'information

RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A1.1 Audit d'un système d'information en sécurité de l'information T1.1 Analyse de maturité d'une organisation en sécurité de l'information T1.2 Proposition de mesures de sécurité pour renforcer la sécurité du système d'information T1.3 Évaluation de la performance des mesures de sécurité & amélioration continue T.1.4 Préparation à l'audit de certification	• C1 Préparer un plan de test (les preuves d'audit à analyser), un plan d'audit et des entretiens pour effectuer un audit de certification en s'appuyant sur ISO 19011 • C2 Effectuer des revues de preuves d'audit (orale & entretiens, documentaire, d'observation, technique, statistique) pour déterminer la conformité de l'organisation en s'appuyant ISO 19011 • C3 Évaluer la performance des mesures de sécurité en place, afin d'optimiser la sécurité du système d'information en s'appuyant sur le NIST SP 800 53 • C4 rédiger un rapport d'audit, pour déterminer le plan d'action afin de renforcer la sécurité du système d'information, par l'application d'une méthodologie d'audit comme ISO 19 011 • C5 Proposer un ensemble de mesures de sécurité, afin de renforcer la sécurité des systèmes d'information, en s'inspirant d'une démarche de type Cycle de Deming • C6 Préparer l'entreprise à une certification en sécurité de l'information, en vue de rassurer les clients et les partenaires, par une démarche d'accréditation à partir d'une norme de certification	**E1. Étude de cas pratique et workshop** Le candidat sera évalué sur sa capacité à mener un audit de maturité en sécurité de l'information. Il s'agit d'une véritable entreprise (anonymisée), qui souhaite se faire certifier ISO 27001 en sécurité de l'information. Les candidats travaillent sur une documentation réelle, fournie en l'état par une entreprise, pour un audit de certification. Ils jouent le rôle d'auditeurs de certification ISO. A partir de la distribution du corpus documentaire, les candidats ont 4 heures pour préparer une présentation PowerPoint de 1h30 devant un jury. Ils doivent notamment répondre aux questions suivantes : - Évaluation de la motivation et des	C1 La planification d'un audit est présenté : plan de test et plan d'audit C2 Des preuves d'audit sont analysées C3 La performance des mesures de sécurité est analysée C4 Un rapport d'audit est rédigé et présente le degré de conformité par rapport aux exigences et des recommandations pour être conforme C5 des propositions de mesures de sécurité sont présentées et argumentées C6 L'entreprise est préparée pour un audit de certification en sécurité de l'information.
A1.2 Audit d'une entreprise et du système d'information en résilience, continuité, gestion de crise et plan de secours	• C7 Préparer un plan de test (les preuves d'audit à analyser), un plan d'audit et des entretiens pour effectuer un audit en résilience, continuité, gestion		C7 La planification d'un audit est présenté : plan de test et plan d'audit

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

T1.5 Analyse de maturité d'une organisation en continuité de l'information, plan de secours et gestion de crise T1.6 Proposition de mesures de sécurité pour renforcer le plan de continuité et de secours T1.7 Évaluation de la performance des mesures de sécurité & amélioration continue T.1.8 Préparation à l'audit de certification	de crise et plan de secours en s'appuyant sur ISO 19011 • C8 Auditer la maturité d'une organisation en termes de continuité et de résilience de l'information (Plan de continuité métier et plan de continuité informatique) pour déterminer les vulnérabilités du système d'information, par l'application d'un ensemble de critères d'audit comme 22301 • C9 Effectuer des revues de preuves d'audit (orale & entretiens, documentaire, d'observation, technique, statistique) pour déterminer la conformité de l'organisation en s'appuyant sur ISO 19011 • C10 Évaluer la performance des mesures de sécurité en place, afin d'optimiser la sécurité du système d'information en s'appuyant sur le NIST SP 800 53 • C11 rédiger un rapport d'audit, pour déterminer le plan d'action afin de renforcer la sécurité du système d'information, par l'application d'une méthodologie d'audit comme ISO 19 011 • C12 Proposer un ensemble de mesures de sécurité, afin de renforcer la sécurité des systèmes d'information, en s'inspirant d'une démarche de type Cycle de Deming • C13 Préparer l'entreprise à une certification en sécurité de l'information, en vue de rassurer les clients et les partenaires, par une démarche d'accréditation à partir d'une norme de certification	enjeux de la direction générale pour faire certifier l'entreprise ISO 27 001 - Identification des menaces, vulnérabilité et impacts en sécurité de l'information - Évaluation des mesures de sécurité mises en place - Évaluation des preuves fournies d'audit (documentaires et techniques) fournies par le client - Rédaction de non-conformités - Évaluation des propositions de traitement des non-conformités par le client	C8 Les vulnérabilités sont présentées C9 Des preuves d'audit sont analysées C10 La performance des mesures de sécurité est analysée C11 Un rapport d'audit est rédigé et présente le degré de conformité par rapport aux exigences et des recommandations pour être conforme C12 des propositions de mesures de sécurité sont présentées et argumentées C13 L'entreprise est préparée pour un audit de certification en sécurité de l'information.
A1.3 Gouvernance des systèmes d'information T1.9 Évaluation de la conformité légale et réglementaire, notamment par rapport au RGPD	• C14 Mettre en place une gouvernance de la sécurité des systèmes d'information, afin de déployer une démarche cohérente au niveau stratégique, tactique et opérationnel, par le déploiement de meilleures pratiques comme Cobit • C15 Évaluer la conformité légale et réglementaires de l'organisation par rapport aux exigences légales et		C14 Le modèle de gouvernance est présenté pour impliquer aussi bien la direction générale que les équipes opérationnelles en termes de protection de l'information. Les règles d'éthique sont appliquées lors d'un entretien de simulation

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE

T1.10 Due Care & Due diligence T1.11 Prise en compte de la propriété intellectuelle T1.12 Protection des données à l'international avec des clients et des fournisseurs en dehors de l'union européenne T1.13 Prise en compte de l'éthique professionnelle dans le monde du hacking	réglementaires en termes de sécurité de l'information et de protection des données personnelles (RGPD), afin d'éviter toute non-conformité et sanctions financières en résultant		C15 Un rapport de non-conformité légales est présenté, ainsi que les solutions pour traiter les non-conformités.

Bloc de spécialisation n°3 – Détecter et traiter les incidents techniques à l'aide de l'intelligence artificielle			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A1 Installer un outil de SIEM (Security Incident & Event Management) T.3.1 Découverte des capacités d'un outil de SIEM de type QRadar T3.2 Prise en main d'un outil de SIEM	• C1 Appliquer les meilleurs pratiques de réponse aux incidents, pour pouvoir intégrer une équipe de SOC (Security Operation Center) ou un CERT (Computer Emergency Response Team) et gérer tout incident de sécurité de l'information (y compris les fuites de données ou DLP Data Leakage Prevention), en appliquant des normes comme ISO 27 035 (gestion des incidents) ou de réponse à gestion de crise	**E1. Étude de cas pratique et workshop** Les candidats sont mis en situation réelle. Ils disposent de 72 heures pour traiter une série d'incidents de sécurité est une fuite de données. Face à un outil de SIEM, ils doivent : - Montrer qu'ils en maîtrisent l'interface, et qu'ils sont capables de repérer des incidents de sécurité et les traiter dans les délais - Appliquer les techniques de recherche avancées (Indexation, corrélation statistique, langage de programmation, etc.) pour repérer une fuite de données et y remédier - Présenter un rapport de suivi de la sécurité de l'information à une équipe technique et un	C1 Un outil de SIEM est utilisé pour repérer des incidents de sécurité et les traiter
A1.2 Analyse et recherche d'anomalies de sécurité T3.3 Enquêter sur les actions suspectes en sécurité T3.4 Filtrer, grouper et analyser les informations de sécurité avec les outils de corrélation de type Splunk	• C2 Utiliser un outil de SIEM (Security Incident & Event Management) du marché, pour repérer une fuite de données (notamment par l'utilisation du machine learning et de l'intelligence artificielle), afin de prévenir celle-ci et d'en limiter les conséquences • C3 Utiliser un outil de type Splunk pour effectuer des corrélations statistiques et des index de données agrégées, pour repérer une série d'incidents de sécurité, ou une fuite de donnée, afin d'y remédier au plus vite		C2 Une fuite de données est repérée, confinée et résolue à partir de l'outils de SIEM et de corrélation statistique C3 Un incident de sécurité est repéré à partir d'un outil de type Splunk et une analyse prédictive basée sur de l'intelligence artificielle
A1.3 Paramétrage d'un outil de SIEM et recherches avancées T3.5 Utilisation des fonctions avancées d'un outil de SIEM : filtrage, programmation de scripts avancés	• C4 Créer des règles pour examiner de façon précise les infractions de sécurité, et utiliser le langage AQL (Ariel Query Language) pour des recherches avancées, pour des analyses de sécurité plus poussées afin d'anticiper les risques de cybersécurité		C4 Des incidents de sécurité furtifs sont repérés grâce à l'utilisation des paramètres avancés d'un outil de SIEM et la création de règles spécifiques
A1.4 Reporting à une équipe technique et à la directon du suivi de la sécurité	• C5 Présenter un rapport de suivi de la sécurité de l'information à une équipe technique et à la		C5 Un rapport technique de suivi de la sécurité est présenté. Ainsi qu'un

T3.6 Présentation d'un rapport de suivi de la sécurité de l'information	direction, pour informer en temps réel du suivi de la sécurité, de mesures mises en place et des risques	autre rapport à la direction	rapport de gouvernance adressé à la direction générale.