INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

Spécialiste en Cybersécurité (MS)

INSA Lyon

Référentiel d'activités, de compétences et d'évaluation

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.* »

La certification Spécialiste en Cybersécurité (MS) est structurée en 3 blocs de compétences :

- Bloc 1 : Définir la Stratégie et la Gouvernance de la sécurité de l'information
- Bloc 2 : Concevoir et mettre en service les infrastructures de cybersécurité
- Bloc 3 : Maintenir en continuité de service

Les évaluations majeures concernant cette certification comprennent des évaluations collectives et individuelles, écrites et orales :

- Des mises en situation professionnelle simulées à partir d'études de cas d'entreprise, comprenant des soutenances orales et/ou des remises de livrables (dossier de veille, note de cadrage, cahier des charges, dossiers de conception et de spécifications fonctionnelles et techniques, prototypes, démonstrations…)
- Des projets avec jeux de rôles réalisés par équipe de 2, puis de 4 à 6 personnes
- Des examens individuels, avec questions et exercices pratiques

L'obtention de la totalité de la certification résulte de la validation complète de tous les blocs de compétences et de la rédaction et soutenance réussies d'une thèse professionnelle.

La thèse professionnelle fait suite à une mission en entreprise qui dure 4 mois minimum. La rédaction de la thèse et sa soutenance constituent une évaluation requise pour l'obtention de la certification, conformément aux directives de la Conférence des Grandes Ecoles. Sont attendus de la part de l'apprenant :
Pour le rapport : les points ci-dessous sont évalués selon des critères de qualité de l'écrit, de complétude, d'argumentation, d'analyse et de synthèse.
Le rapporteur du mémoire dispose d'un formulaire détaillé qui permet d'évaluer chacun de ces points :

- Présentation du contexte de la mission professionnelle (économique, organisationnel, technique, concurrence, alliances etc.)
- Description des activités réalisées (objectifs, réalisations effectuées, méthodologie, planning, difficultés, succès etc.)
- Problématique de recherche (portée, intérêt, bibliographie, méthodologie, résultats, conclusions et recommandations)
- Synthèse de la thèse (analyse critique, suggestions et recommandations, plan de carrière etc.)

Pour la soutenance : le jury dispose d'un formulaire détaillé pour évaluer la présentation selon les critères de qualité de l'oral et du support, de pertinence des réponses apportées, de prise de recul, de capacité de synthèse.

Une validation de la certification est aussi possible dans le cadre d'une procédure VAE : recevabilité, livret 2, soutenance orale et validation par un jury. Une VAE hybride est également possible.

Les élèves en situation de handicap peuvent s'adresser à l'Institut Gaston Berger de l'INSA Lyon pour la prise en compte de leur situation. https://institut-gaston-berger.insa-lyon.fr/fr/content/handicap

Une intervention de la cellule handicap de l'Institut Gaston Berger de l'INSA Lyon est inclue dans la formation. Intitulée « Le handicap, qu'est-ce que c'est ? », elle permet à la fois de connaître le cadre légal et les différents types de situations et d'apporter des réponses à la problématique de sa prise en compte dans le cadre d'une équipe professionnelle, en situation de travail ou de management d'un collaborateur en situation de handicap.

REFERENTIEL D'ACTIVITES	REFERENTIEL DE COMPETENCES	REFERENTIEL D'EVALUATION MODALITES d'EVALUATION	REFERENTIEL D'EVALUATION CRITERES D'EVALUATION
Bloc de Compétences n°1 : Définir la Stratégie et la Gouvernance de la sécurité de l'information			
A11- Élaboration du Système de Management de la Sécurité du Système d'Information (SMSI)	• C1.1.1-Définir le périmètre d'application et la politique de sécurité, afin de recenser les actifs informationnels et supports sur lesquels doit porter une démarche d'appréciation des risques et les principes d'action de la politique de sécurité de l'information, grâce au contexte de l'organisation établi et validé par la direction générale. • C1.1.2-Identifier, apprécier et définir les seuils d'acceptabilité des risques sur le périmètre, afin d'établir un plan de traitement des risques grâce à une méthodologie d'appréciation du risque en concordance avec les objectifs de la politique de sécurité de l'information de l'organisme mais aussi du cadre normatif. • C1.1.3-Choisir et piloter la mise en place des mesures de sécurité techniques et organisationnelles, afin de réduire ou supprimer des risques, en allouant les moyens budgétaires et humains qui permettront la mise en œuvre effective des fonctions adéquates de sécurité • C1.1.4-Contrôler le SMSI dans une boucle d'amélioration continue, technique, financière et organisationnelle, afin d'éclairer les choix stratégiques à opérer en matière de sécurité, par la mise en place d'indicateurs pertinents sur le périmètre d'analyse. • C1.1.5-Piloter les différents projets liés à la définition et mise en œuvre du SMSI, afin que le niveau de maturité en cybersécurité	Des **exercices théoriques et pratiques** permettant d'illustrer chaque étape. A l'issue d'une période de réflexion, un corrigé est fait par l'intervenant, ce qui permet à chaque apprenant de s'auto-évaluer **Étude de cas** : Définition et mise en place du SMSI, dans une organisation selon la norme iso27001 Lead implementer. Les participants sont organisés en groupes projet de 5 personnes au maximum. Ils doivent produire une restitution finale (support écrit et soutenance orale) argumentée en groupe devant l'intervenant professionnel et l'ensemble des participants, avec un livrable portant sur • Périmètre du SMSI • Identification des fonctions de sécurité • Identification et plan de traitements des risques • Choix des mesures de sécurité • Intégration des mesures de sécurité dans l'architecture existante	• Cr1(C1.1.1)-Le périmètre du SMSI est en cohérence avec les activités sur lesquelles il s'applique • Cr2((C1.1.2)-Les besoins en sécurité sont correctement identifiés sur le périmètre du SMSI • Cr3(C1.1.2)-L'identification et le traitement des risques sont en cohérence avec le périmètre du SMSI • Cr4(C1.1.3)-Les mesures de sécurité choisies sont justifiées et s'intègrent dans l'infrastructure existante • Cr5(C1.1.4)-Les indicateurs choisis permettent de contrôler les fonctions de sécurité sur le périmètre d'analyse • Cr6(C1.1.5)-Le budget et les ressources allouées aux projets sont suffisantes et justifiées • Cr7(C1.1.5)-Les actions d'amélioration du SMSI sont

	de l'organisation soit en phase avec ses choix stratégiques et orientations business, par la mise en œuvre de capacités comportementales tel que leadership, rigueur, sens relationnel, travail en équipe inclusive, gestion du stress, communication orale et écrite, analyse et synthèse, respect des délais et des budgets.	• Budget et ressources allouées au projet • Indicateurs choisis pour le périmètre SMSI • Actions d'amélioration du SMSI (risques résiduels) • Phasage du projet SMSI	correctes et conduisent à élever le niveau de maturité en cybersécurité) • Cr8(C1.1.5)-Les phases du projet sont correctement identifiées • Cr9 (C1.1.5) Les capacités comportementales permettent un pilotage efficace des projets
A12-Gouvernance et gestion des accès et des identités	• C1.2.1-Identifier tous les accès internes et externes existants aux actifs (réseaux, systèmes, applications, données), afin de prendre en compte les différents environnements d'utilisateurs Interne, cloud et fédérés par la mise en œuvre d'un audit préalable auprès des responsables d'application • C1.2.2-Implémenter et gérer les mécanismes d'autorisation afin de prendre en compte l'évolution des accès par la mise en œuvre de modèles de contrôle des accès, dans une matrice des rôles du ressort des managers des directions métier • C1.2.3-Gérer le cycle de vie des identités et du provisionnement des accès, afin de réaliser des revues des accès des utilisateurs, comptes d'accès système, provisionnement et dé-provisionnement • C1.2.4-Choisir des solutions de gestion des accès et des identités adaptées au contexte et besoins, afin de mettre en place des architectures IAM (Identity Access Management) , techniques et fonctionnelles, par la mise en œuvre et le déploiement sur les systèmes de fonctions tel que fédération des identités, Single Sign on, gestion des comptes privilégiés etc.	**Étude de cas** : Définition et mise en place d'une gestion des identités avec plateforme logicielle, dans une organisation. Les participants sont organisés en groupes projet de 5 personnes au maximum. Ils doivent produire une restitution finale (support écrit et soutenance orale) argumentée en groupe devant l'intervenant professionnel et l'ensemble des participants, avec un livrable portant sur : • Définition des identités et des accès internes et externe aux ressources de l'organisation • Plan du cycle de vie des identités selon les métiers avec définition des habilitations • Démarche de création et provisionnement de la base de données des identités • Architecture technique et fonctionnel de la solution de gestion des accès	• Cr1 (1.2.1)-La définition des identités et des accès internes et externe aux ressources de l'organisation recouvre l'ensemble des métiers • Cr2(C1.2.2)- les modèles de contrôle des accès sont identifiés dans une matrice des rôles • Cr3(1.2.3)-Le plan du cycle de vie permet la prise en compte de l'évolution des accès des utilisateurs au sein de leur organisation afin de garantir l'attribution des bons droits aux bonnes personnes, et faciliter les audits des habilitations informatiques • Cr4(C1.2.4)- la solution IAM retenue couvre les besoins techniques et fonctionnels

	• C1.2.5 - Analyser les données liées aux identités, aux comptes et leurs habilitations applicatives afin de les faire évoluer par la mise en œuvre d'un outillage logiciel • C1.2.6-Piloter les différents projets sur la gestion des accès et des identités, afin de permettre à l'organisation de contrôler de manière stricte qui accède à quel actif informationnel et dans quel but ? Par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets.	**Travaux pratiques** : sur mise en œuvre d'une solution de gestion des accès. Les apprenants devront fournir rendre individuellement à l'intervenant un livrable qui consiste en des copies d'écran commentées de la démarche d'installation et d'utilisation.	• Cr5(C1.2.5)-La création et la structuration de l'annuaire recensent effectivement les ressources et utilisateurs ayant des droits et autorisations d'accès • Cr6(C1.2.6)-La configuration, la mise en place et les tests de différentes méthodes d'accès (mots de passe, identification unique, environnement de confiance entre deux systèmes, accès selon rôle etc.) sont un succès • Cr7(C1.2.6) Les capacités comportementales permettent de piloter efficacement les projets
A13-Analyse et cartographie des risques en sécurité de l'information selon la méthodologie EBIOS RM (Risk manager)	• C1.3.1-Identifier et analyser les sources de risques, dans une approche orientée stratégie cybersécurité de l'organisation, politique de gestion des données et des traitements pour vérifier la conformité à la loi (protection des données, loi défense, loi de programmation militaire, …), afin d'identifier ceux qui pourraient nuire à l'organisation, par la mise en œuvre de l'atelier 2 de la méthodologie EBIOS RM (Sources de risques). • C1.3.2-Identifier l'ensemble des parties prenantes internes et externes (partenaires, sous-traitants, filiales, etc.) de l'organisation, afin de lister les probables chemins d'attaque via les parties prenantes par la mise en œuvre de l'atelier 3 de la méthodologie EBIOS RM (Scénarios stratégiques).	**Étude de cas** : Analyse et gestion des risques dans une organisation selon la méthodologie EBIOS Risk manager. Les participants sont organisés en groupes projet de 5 personnes au maximum. Ils doivent produire une restitution finale (support écrit et soutenance orale) argumentée en groupe devant l'intervenant professionnel et l'ensemble des participants, avec les livrables suivants : • Sources de risques sur le périmètre d'analyse • La matrice des rôles	• Cr1(C1.3.1)- Identification des sources de risques sur le périmètre d'analyse est correcte • Cr2(C1.3.2)-La matrice des rôles et responsabilités qui permet de planifier les étapes de l'analyse ainsi que les personnes impliquées dans chaque atelier est cohérente avec le périmètre d'analyse • Cr3(C1.3.2)-La détermination des valeurs métiers qui représentent les processus et informations métiers du périmètre d'analyse,

	• C1.3.3-Identifier les chemins d'attaque à partir d'actions élémentaires sur les biens supports (systèmes, réseaux, bases de données etc.) afin d'estimer leurs vraisemblances, par la mise en œuvre de l'atelier 4 de la méthodologie EBIOS RM (Scénarios opérationnels) • C1.3.4-Définir une stratégie de traitement du risque, afin de décliner les Mesures de sécurité et un plan d'amélioration continue par la mise en œuvre de l'atelier 5 de la méthodologie EBIOS RM. (Traitement du risque) tout en respectant les différentes règlementations en vigueur sur la protection des données (RGPD, CNIL) • C1.3.5-Piloter les différents projets sur le traitement des risques, afin de permettre à l'organisation d'exercer ses activités par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets.	• La liste des biens supports et responsables adéquats • Différents tableaux (sources de risques, effets recherchés par les assaillants, scénarios opérationnels) • Matrice des risques : Établissement d'une matrice des risques en se basant sur la gravité et la vraisemblance des scénarios • Plan de traitement des risques avec prise en compte des différentes règlementations (RGPD, CNIL)	permet d'identifier, les biens supports et les responsables adéquats • Cr4(C1.3.3)Le tableau de mise en correspondance entre les sources de risques et les effets recherchés par les assaillants, permet d'avoir une vision claire sur la pertinence des évènements redoutés • Cr5(C1.3.3) Les scénarios techniques et modes opératoires permettant la réalisation effective des scénarios opérationnels sont vraisemblables • Cr5(C1.3.4) La conformité aux règlementations (RGPD, CNIL) est correcte • Cr6(C1.3.5) Le plan de traitement des risques, contribue effectivement à la réduction des risques • Cr7(C1.3.6) Les capacités comportementales permettent de piloter efficacement le projet

BLOC DE COMPETENCES N°2 : Concevoir et mettre en service les infrastructures de cybersécurité			
A21- Conception et mise en œuvre de la sécurisation d'une Infrastructure IT (réseaux, systèmes, applications)	• C2.1.1-Concevoir une architecture qui prend en compte les enjeux et contraintes techniques, organisationnelles, règlementaires et financières de l'organisation/entreprise, afin de construire une architecture durable, performante et évolutive. • C2.1.2-Intégrer au mieux les différents équipements et solutions de sécurité du marché (veille technologique approfondie), afin de prendre en compte le contexte propre à l'organisation par la mise en œuvre de techniques de déploiement et de migration compatibles avec le contexte et le cadre règlementaire. • C2.1.3-Conseiller et/ou convaincre un donneur d'ordre (autorité, chef de projet, chef DSI...), afin de mobilier les ressources budgétaires et humaines pour réaliser le projet de sécurisation • C2.1.4-Piloter les différents projets sur la conception et mise en œuvre des fonctions de sécurité, afin de permettre à l'organisation de protéger son infrastructure par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets.	**Étude de cas** : Appel d'offres d'une entreprise qui souhaite sécuriser son infrastructure. Travail réalisé sur trois jours en mode projet avec soutenance argumentée par chaque groupe de la réponse à l'appel d'offres. Le livrable de soutenance porte sur : - Prise en compte du contexte de l'organisation - Une architecture qui couvre les besoins en cybersécurité de l'organisation - Le projet de déploiement de l'architecture avec mise en évidence des différentes phases : Étude/intégration/Tests - Un descriptif des produits et solutions de sécurité à installer - Une évaluation économique des équipements et prestations de service - Un courrier destiné aux décideurs rappelant les enjeux du projet Rapport de travaux pratiques sur sécurité des réseaux sans fils et Objets connectés	• Cr(C2.1.1 et C2.1.3)-Démonstration de la viabilité technico-économique des architectures, du niveau d'adéquation, avec le besoin exprimé, justification pertinente des choix effectués • Cr(C2.1.2)-Les mécanismes de sécurité et leurs interactions sont bien identifiés • Cr(2.1.2)-Les produits et solutions décrites sont en cohérence avec les contraintes économiques et règlementaires de l'organisation • Cr(2.1.2)-Configurations réussies des différentes fonctionnalités de sécurité (filtrage, VPN, authentification, certificats etc.) • Cr(2.1.2)-Les failles des applications sont identifiées et les actions correctives mises en Œuvre agissent bien sur les causes racines du problème et permettent de constater un fonctionnement normal de l'application

		Rapport de travaux pratiques sur infrastructure PKI (Public Key Infrastructure) Rapport de travaux pratiques sur audit d'applications et de tests de codes applicatifs.	• Cr(C2.1.2)-La démarche d'analyse du code permet d'identifier les vulnérabilités • Cr(C2.1.4)-Les tâches du projet, leurs durées et des moyens humains nécessaires sont corrects et réalistes • Cr(C2.1.4) Les capacités comportementales permettent de piloter efficacement le projet
A22-Étude et Intégration de la sécurité dans le processus de développement d'un produit industriel complexe (Train, Avion etc)	• C2.2.1-Réaliser les études de sécurité dans le cadre d'un développement de produit industriel afin d'identifier les fonctions de sécurité qui permettront à l'utilisateur d'opérer ce produit en sécurité, en intégrant les étapes classiques de la sécurité (analyse de risque, réduction des risques par intégration des mesures de sécurité, évaluation) au cycle de développement du produit. • C2.2.2-Identifier, adapter et intégrer les activités de gestion des risques dans le processus de développement d'un produit industriel complexe (avion, train, etc. …) par la mise en œuvre de méthodologies adaptées (analyse de code) afin de mettre en conformité son niveau de sécurité. • C2.2.3-Évaluer les informations de sécurité attendues et le niveau de maturité à chaque étape du processus de développement afin d'établir le niveau de sécurité du produits et les risques résiduels à l'issue de la phase d'intégration finale du produit.	**Étude de cas en fil rouge du cours :** Étude d'un modèle simplifié de navette ferroviaire, et présentation par groupe d'un livrable sur les étapes du processus d'étude et d'intégration de la sécurité : • Identification des fonctions principales et impacts en CID (confidentialité, Intégrité Disponibilité) associés • Proposition d'une architecture de sécurité sur base de l'architecture de la navette • Définition des Scénarios de menace • Évaluation des risques associés • Gestion d'un changement • Sélection des COTS[1] dans le cadre du développement.	• Cr(C2.2.1)-Les fonctions principales de sécurité identifiées sont en rapport avec le périmètre d'étude • Cr(C2.2.1)-L'architecture technique proposée intègre les fonctions de sécurité • Cr(C2.2.2 et C2.2.3)-Les scénarios de menace sont identifiés et les risques principaux et résiduels évalués • Cr(C2.2.4)-Le processus de gestion des changements permet de maintenir un bon niveau de sécurité lors de l'évolution du produit

[1] COTS : commercial off-the-shelf (Les produits COTS sont conçus pour être facilement installés et pour interagir avec les composants système existants)

	• C2.2.4-Identifier et adapter le processus de gestion du changement du produit afin de maintenir le niveau de sécurité du produit à travers son évolution. • C2.2.5-Définir et mettre en œuvre un système d'assurance sécurité pour garantir l'atteinte des objectifs de sécurité dans la supply chain.		• Cr(C2.2.5)-Les produits COTS sont facilement installables

BLOC DE COMPETENCES N°3 : Maintenir en continuité de service			
A31-Réalisation de tests d'intrusion	• C3.1.1-Définir et analyser le périmètre d'intervention afin d'y rechercher des vulnérabilités par une recherche directe ou indirecte d'informations sur l'organisation cible (services accessibles, infrastructure) • C3.1.2-Réaliser des audits de type tests d'intrusion, audit de code, audit de configuration etc. afin d'identifier et qualifier les vecteurs de risques (défauts de configuration, ports ouverts, code non sécurisé etc.), par l'élaboration, et la planification de scénarios d'attaques • C3.1.3-Rédiger pour les métiers, un rapport d'analyse des vulnérabilités découvertes afin de préconiser des mesures correctives, fournir des preuves, rendre compte et documenter • C3.1.4-Réaliser des analyses post-mortem (Forensic) afin d'adapter la campagne de tests par l'intégration dans ses propositions des exigences des différents types d'investigation (administratives, criminelles, civiles, règlementaires) • C3.1.5-Piloter les différents projets sur la conception et mise en œuvre des tests d'intrusion, afin de permettre à l'organisation de protéger son infrastructure, par la mise en œuvre d'une conduite	**Travaux pratiques en fil rouge** : Portant sur la mise en œuvre de tests techniques d'intrusion sur réseau, applications web et analyse Forensic Les apprenants se connectent individuellement sur une plateforme applicative fournie par l'intervenant. Un compte rendu est demandé pour chaque groupe de 3/4 apprenants. Le rapport décrit : - Démarche de recherche de vulnérabilités et l'outillage associé - Création de scénarios d'attaque et typologie des tests à réaliser - La réalisation effective des attaques - Une synthèse sur les principales vulnérabilités découvertes - L'analyse Forensic **Examen** sur la même plateforme que les travaux pratiques, individuellement en temps limité (3h) avec un challenge différent	• Cr(C3.1.1)Le périmètre d'audit technique interne et externe est correctement identifié et est cohérent avec l'environnement de la plateforme • Cr(3.1.2)-La démarche de recherche de vulnérabilités est décrite en détail (type de tests, types d'audit, défauts de configuration…) . • Cr(3.1.2)-Les scénarios d'attaque choisis sont réalistes • Cr(3.1.2)-Réalisation aboutie des tests d'intrusion et d'investigation • Cr(C3.1.3)-Analyse pertinente des résultats et proposition de

	de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets.		mise en place des bonnes remédiations • Cr(C3.1.4)- Les preuves numériques réunies sont utilisables , dans le cadre d'une enquête judiciaire • Cr(C3.1.5)- Les tâches du projet, leurs durées et des moyens humains nécessaires sont correctes et réalistes • Cr(C3.1.5) Les capacités comportementales permettent de piloter efficacement le projet
A32-Mise en place du plan de continuité et de Reprise d'activité (PCA/PRA)	• C3.2.1-Procéder à une classification des applications et serveurs afin d'identifier ceux qui sont critiques, et prévoir leur continuité de fonctionnement, par un questionnement structuré avec les métiers, des visites sur site, des réunions, des tests d'intrusion, un examen des documents existants (politiques, chartes etc.) • C3.2.2-Définir avec les métiers et la direction des systèmes d'information la continuité de service, pour les applications et serveurs critiques, afin de garantir un fonctionnement normal, par l'estimation des critères de continuité de service (durée d'interruption maximal du service, perte de données maximum admissible etc.) • C3.2.3-Définir une organisation afin de gérer le plus efficacement possible un sinistre par la mise en œuvre d'une équipe dédiée PCA/PRA	**Étude de cas** : Étude d'un plan PCA/PRA pour une organisation. Les participants sont organisés en groupes projet et doivent produire une restitution finale (Rapport et soutenance) argumentée devant l'intervenant professionnel et l'ensemble des participants, avec un livrable portant sur : • Classification de la criticité des actifs selon les critères CDI (Confidentialité, Disponibilité, Intégrité) • Estimation des critères de mesure de la continuité de service • Choix des mesures afin de réduite l'impact et la potentialité des sinistres	• Cr(C3..1)-Les actifs critiques sont identifiés et classifiés selon les critères CDI • Cr(C3.2.2)-Les critères de mesures de la continuité de service sont définis et évalués • Cr(C3.2.2)-La réduction de l'impact et la potentialité des sinistres est effectivement constatée pour chaque mesure choisie • Cr(C3.2.3)-L'organisation de la gestion de crises, identifie clairement, les différents

	• C3.2.4-Identifier les évolutions à apporter au PCA/PRA, afin d'anticiper de futures cyber-crises, en inscrivant le PCA/PRA dans une boucle d'amélioration continue avec la mise en œuvre d'un plan de maintien en condition opérationnelle • C3.2.5-Piloter le projet de PCA/PRA afin de permettre à l'organisation d'augmenter sa résilience, par la mise en œuvre d'une conduite de projet mobilisant des capacités comportementales telles que leadership, rigueur, sens relationnel, travail en équipe inclusive, communication orale et écrite, respect des délais et des budgets.	• Définir l'organisation de gestion de crise (composition, rôles et fonctions, dispositif d'alerte etc.) • Plan de maintien en conditions opérationnelles • Mise en en œuvre d'un PRA cloud. Les apprenants rédigent un compte rendu de TP évalué par l'intervenant professionnel	membres, leurs rôles, les fonctions etc. • Cr(C3.2.4)-Les actions concrètes du plan de maintien en conditions opérationnelles et son évolution sont définies (qui fait quoi quand comment) • Cr(C3.2.4)Le PRA cloud mis en œuvre est opérationnel • Cr(C3.2.5)- Les tâches du projet, leurs durées et des moyens humains nécessaires sont correctes et réalistes • Cr(C3.2.5) Les capacités comportementales permettent de piloter efficacement le projet