Référentiel d'activités, de compétences et d'évaluation

Intitulé du titre postulé :
Expert sécurité des données, des réseaux et des systèmes

Ecole 2600

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
Apporter son expertise SSI aux organes de direction.	Analyser les pratiques professionnelles des collaborateurs afin de proposer des améliorations dans leur application des normes, des standards et du respect du droit relatifs à la sécurité informatique dans les architectures de SI, ou les applications.	Exercices pratiques qui portent sur la conception, puis la rédaction des documents permettant de structurer l'organisation de la sécurité des SI en articulant un aspect sécurité (norme, standard, droit, ...) à la réalité de terrain de l'entreprise). Les documents sont ensuite défendus devant un jury.	Le besoin a été correctement identifié et compris. Les enjeux et les menaces sont clairement et correctement identifiés. Les arguments juridiques correctement identifiés et expliqués. Les normes ont été respectées et sont en adéquation avec le domaine de l'activité de l'entreprise (PCI-DSS, ...). Les argumentations orales sont claires, précises et convaincantes et permettent d'éclairer un COMEX sur les enjeux en cybersécurité.
	Rédiger pour son organisation des notes, des guides, des présentations et/ou des directives d'application afin de réduire le risque en cybersécurité, qui s'appuient		

	sur les éléments identifiés en phase d'analyse.		
	Conseiller son organisation sur l'utilisation et sur la portée stratégique des notes, guides, directives d'application rédigées après l'analyse.		
Élaborer les stratégies de l'organisation dans le domaine de la SSI.	Analyser son organisation afin d'augmenter la cyber résilience de celle-ci, en étudiant les éléments suivants: - Les menaces en cybersécurité relatives à l'activité de l'entreprise; - Le plan de continuité d'activité relatif aux crises cyber sécurités (PCA); - Le plan de reprise d'activité relatif aux crises cyber sécurités (PRA).	Mise en situation au travers d'étude de cas typique d'entreprise au choix (OIV, PMI, TPE, Grand groupe, ...) nécessitant la rédaction d'un PCA (Plan de continuité d'activité) cyber et d'un PRA (Plan de reprise d'activité) cyber soutenu devant jury. Mise en situation au travers d'étude de cas sur les stratégies cybers déployables dans des contextes précis et relatives à un type d'entreprise au choix (OIV, PMI, TPE, Grand groupe, ...). Les stratégies	Le PCA et PRA cyber sont rédigés en adéquation avec le contexte de l'entreprise (complétude et pertinence). Les enjeux et les menaces sont clairement et correctement identifiés. La stratégie défendue est pertinente pour le cas étudié. Les argumentations orales sont claires, précises et convaincantes et permettent à un COMEX de définir une stratégie en cybersécurité.
	Rédiger des notes, des guides, des présentations afin d'éclairer sa hiérarchie et d'augmenter la cyber résilience, qui s'appuient sur les éléments identifiés en phase d'analyse de l'activité.		

		déployées sont soutenues devant jury.	
	Défendre auprès de sa hiérarchie une vision stratégique en cybersécurité afin de prévenir le risque cyber sur le temps long.		
Réaliser une veille technologique sur l'actualité des vulnérabilités, des menaces et des produits dans le domaine de la cybersécurité.	Évaluer les solutions d'analyse de menace et de contre-mesure de type COTS (Component On The Shelf), OSINT (Open Source Intelligence), ou autre applicable sur le SI de l'organisation afin de juger des opportunités d'amélioration de la sécurité des données, des systèmes et du réseaux.	Exercices pratiques qui portent sur la mise en œuvre des techniques d'attaque/défense ou d'outils spécialisés sur une infrastructure de simulation et de correction automatique suivie de l'écriture de compte rendu technique. Mise en situation au travers de projets d'actualité de la cybersécurité afin de juger sa proactivité face à celle-ci. Cette mise en situation fait l'objet d'un rapport écrit expliquant et justifiant les choix de l'innovation apportée et	Les techniques d'attaque/défenses ont été identifiées et utilisées avec pertinence en situation réelle. Les comptes rendus techniques sont évalués sur leur facilité de compréhension (référence et mise en perspective de l'information) au sein d'une organisation afin de constituer un fond documentaire sur la mise en pratique réelle des techniques utilisées. Les rapports de projet d'actualité sont évalués sur
	Analyser les évolutions technologiques en cybersécurité (techniques d'attaque et de défense logiciels, matériels ou sociales) afin de maintenir son niveau d'expertise dans le domaine et d'identifier de "nouveaux" risques potentiels.		

	Participer aux innovations de la sécurité des SI publiés officiellement sur les canaux spécialisés (conférence, podcast, blog, ...) afin d'augmenter son expertise sur les potentiels risques pour le SI de l'organisation et mieux identifier de nouvelles attaques cyber.	sera soutenue oralement devant jury.	la qualité et l'adéquation des solutions apportées.
Concevoir des solutions informatiques de façon sécurisée.	Concevoir l'architecture SI de l'entreprise dans le contexte d'un réseau informatique, télécom ou industriel afin de répondre au besoin fonctionnel de l'organisation en prenant en compte le plan de routage, le cloud, la localisation des services, le besoin exprimé de fonctionnalité du SI.	Exercices pratiques qui portent sur la conception et la mise en œuvre d'un projet informatique (SI, application, ...) respectant l'application des bonnes pratiques en sécurité informatique. Mise en situation au travers de projets informatiques complets et concrets respectant toutes les consignes de production sécurisée: - Infrastructure SI partiel ou complète - Applications (standard, web, embarquée, ...) d'une entreprise répondant à une	Les projets proposés (architectures, applications, solutions) répondent aux besoins exprimés, et aux contraintes de sécurité. Les rapports de projet sont évalués sur la qualité et l'adéquation des solutions apportées, leurs applications concrètes et pratiques. Les prestations orales sont claires, précises et convaincantes et permettent d'identifier que le candidat est à même d'animer ou
	Mettre en œuvre l'architecture SI de l'entreprise dans le contexte d'un réseau informatique, télécom ou industriel afin de rendre opérationnelles les nouvelles fonctionnalités en prenant en		

	compte les solutions logicielles de déploiement d'architecture (ansible, puppet, ...) et les spécificités des systèmes visées (windows, linux, ...).	expression de besoin. Cette mise en situation fait l'objet d'un rapport écrit expliquant et justifiant les choix de la solution apportée (en intégrant la composante sécurité) et sera soutenue oralement devant jury.	participer à une conférence ou à un podcast.
	Concevoir des solutions logicielles de façon sécurisée dans les contextes d'une application lourde, du web ou de l'embarqué afin de répondre aux besoins fonctionnels du produit visé en fonction des problématiques algorithmique, de performance, de l'architecture du code, et les interactions avec les bases de données.		
	Mettre en œuvre les solutions logicielles de façon sécurisée dans les contextes d'une application lourde, du web ou de l'embarqué afin de rendre opérationnelles les nouvelles fonctionnalités en prenant en compte les spécificités des		

	langages employés, des bibliothèques de fonctions, et des API de services tiers.		
Auditer la sécurité informatique.	Contrôler la bonne application des notes, recommandations, guides et/ou des directives d'application rédigées/exprimées pendant l'activité de conseil concernant: - La conception et le développement sécurisé d'applications lourdes, web ou embarquées. - En conception et mise en œuvre d'architecture sécurisée de système d'information sur le SI de l'organisation.	Exercices pratiques qui portent sur l'investigation technique d'un projet informatique (SI, application, …) afin de contrôler la présence ou l'absence de faille exploitable à des fins malveillantes soit manuellement, soit par des outils. Mise en situation au travers d'étude de cas nécessitant la réalisation d'un Audit sécurité soutenus devant un jury.	Les comptes rendus d'audit de sécurité sont évalués sur la qualité des prescriptions. Elles doivent être adaptées aux réalités (temps/coûts) de l'entreprise, et se montrer techniquement pertinentes. Ils mettent en évidence les écarts constatés et passent en revue les méthodes et moyens (outils) employés pour les trouver.
	Analyser les écarts entre les recommandations rédigées/exprimées pendant l'activité de conseil et la mise en œuvre technique afin d'établir des points de contrôle en utilisant les techniques d'attaques informatiques et les outils associés.		

Prévenir une crise en cybersécurité tout en permettant la continuité et/ou la reprise d'activité.	Contrôler l'application par le personnel en charge du SI de l'entreprise des éléments cyber du PCA et du PRA afin de permettre respectivement la continuité et la reprise d'activité.	Mise en situation au travers d'étude de cas portant sur l'analyse de PCA (Plan de continuité d'activité) cyber et de PRA (Plan de reprise d'activité) cyber sur lequel il faut identifier les points de contrôles dans l'organisation, planifier les missions des équipes techniques pour la mise en conformité , synthétiser le tout dans un rapport soutenus devant un jury.	Les points de contrôles ont été identifiés et leurs pertinences argumentées. Les planifications établies sont réalistes par rapport aux cas étudiés.
	Planifier les missions des équipes techniques concernant l'application des éléments cyber du PCA et du PRA afin de permettre respectivement la continuité et la reprise d'activité.		
Gérer une crise de cybersécurité en lien avec les équipes techniques.	Evaluer les équipes techniques afin de réduire le risque en cybersécurité sur leur compréhension et leur application des notes, recommandations, guides et/ou des directives d'application rédigées/exprimés pendant l'activité d'audit	Exercices pratiques en groupe sur le management humain, la prise de décision, le développement des "soft-skills" via des jeux de rôle. Mise en situation au travers de projets informatiques de groupe complets et concrets respectant toutes les	Le délai imparti est respecté. Les bonnes pratiques en sécurité informatique sont utilisées de manière adéquate pour prévenir d'éventuelles failles exploitables. Les techniques d'attaque/défenses ont été identifiées et utilisées
	Piloter les équipes techniques en situation de crise de cybersécurité afin d'apporter,		

	par son expertise, la capacité de réagir rapidement et de s'adapter aux imprévus non couverts par les documents préventifs préalablement établis (PCA,PRA, autres...)	consignes de production sécurisée: - Infrastructure SI partiel ou complète - Applications (standard, web, embarquée, ...) d'une entreprise répondant à une expression de besoin. Mise en situation au travers de compétitions en équipe de sécurité chronométrées de type CTF (Capture the Flags) Jeopardy et/ou en Red/Blue team (attaque/défense) suivie de l'écriture de compte rendu technique et situationnel sur le déroulement du concours.	avec pertinence en situation réelle. Les comptes rendus techniques de CTF sont évalués sur la description de la démarche employée par le candidat et sur la pertinence technique afin de constituer un fond documentaire sur la mise pratique réelle des techniques utilisées. Le compte rendu de CTF ou de crise du candidat fait apparaître les forces et faiblesses de sa gestion de crise. Les contraintes de continuité et les délais de reprise d'activité impartis sont respectés. Les prestations orales sont claires, précises et convaincantes.
	Contrôler l'application des consignes de sécurité émises en phase conseil et lors de retour d'expérience à destination des équipes techniques afin de se préparer à une crise cyber.		
Assurer la capitalisation des retours d'incident en mesure	Analyser, en situation de crise de cybersécurité, les écarts	Mise en situation au travers de scénario de	Le délai imparti est respecté.

préventive et/ou corrective dans le PCA, le PRA, le SI ou la production.	entre les documents préventifs préalablement établis (PCA, PRA, autres...) et les incidents rencontrés afin d'alimenter le retour d'expérience. Rédiger un retour d'expérience sur les incidents rencontrés en crise cyber afin de maintenir et faire évoluer tous les documents préventifs préalablement établie (PCA, PRA, autres...).	crise (type red/blue team), de cas typique d'entreprise au choix (OIV, PMI, TPE, Grand groupe) nécessitant la mise en application d'un PCA (Plan de continuité d'activité) cyber puis d'un PRA (Plan de reprise d'activité) cyber. Suivie de l'écriture de compte rendu technique et situationnel sur le déroulement de la crise soutenu devant jury.	Les comptes rendus techniques de la crise sont évalués sur leur facilité de compréhension (référence et mise en perspective de l'information) au sein d'une organisation afin de constituer un fond documentaire sur la mise en pratique réelle des techniques utilisées et sur comment s'en prémunir. Le compte rendu de crise du candidat fait apparaître les forces et faiblesses de sa gestion de crise. Les contraintes de continuité et les délais de reprise d'activité impartis sont respectés. Les prestations orales sont claires, précises et convaincantes.

Créer une entreprise innovante dans le domaine de la SSI.	Analyser l'écosystème cyber via une étude de marché afin d'identifier des opportunités de création d'entreprise.	Mise en situation par la rédaction d'une analyse technologique du marché de la sécurité et des opportunités de création d'entreprise. Mise en situation par la rédaction d'un Business Plan pour une entreprise type "moonshot" et d'un Lean Canevas. Mise en situation par la rédaction d'un support de présentation investisseur complet ainsi que pour BPI France. Mise en situation par la rédaction d'une roadmap de financement et d'un document d'impact sur la société (valorisation, montants levés, effet de levier, impacts sur la gouvernance et sur les relations entre actionnaires).	L'analyse de marché proposée identifie les éléments business et technologiques de la concurrence. Le Business Plan répond aux dix critères d'évaluation suivants: rentabilité, adéquation homme/projet, adéquation produit/marché, innovation, faisabilité technique, création d'emploi, cohérence, pertinence, pérennité, apport personnel. Le Lean Canevas reprend le problème, la solution, l'indicateur de performance, la proposition unique de valeur, l'avantage compétitif, les canaux d'acquisition marketing, les segments de clientèle, les coûts et les sources de revenus. La présentation investisseur identifie la
	Concevoir un lean canevas et business plan prenant en compte les éléments financiers prévisionnels, les opportunités du marché, les éléments commerciaux et marketing afin de convaincre de la solidité du projet auprès des futurs investisseurs.		
	Définir une stratégie d'investissement conforme avec le business plan en prenant en compte la valorisation du projet et le cycle de financement (amorçage, dispositifs de BPI France, fonds d'investissements) afin de convaincre des partenaires de financer le projet.		
	Définir une stratégie marketing et commerciale pour adresser les clients potentiels grâce à des canaux de distribution, une		

	stratégie de prix compétitif et un CRM performant en accord avec le business plan.	Mise en situation par la rédaction d'une stratégie d'acquisition marketing permettant le sourcing de prospects puis leur transformation commerciale dans le respect du business plan. Exercices pratiques sur les activités courantes de la gestion d'entreprise: comptes de résultat, bilan, tableau de flux, indicateurs-clés de performance.	raison d'être, le problème adressé, la solution, le pourquoi maintenant, la taille de marché, le produit, l'équipe, le modèle économique, la compétition et la projection financière La stratégie marketing et commerciale identifie les canaux d'acquisitions (growth marketing, acquisition payante etc.), l'argumentaire de vente, le traitement des objections ainsi que les outils nécessaires à mettre en place (CRM, outils marketing…) Au regard des exercices sur les activités courantes de gestion, les candidats sont évalués sur leur capacité à relier les éléments opérationnels et leurs conséquences financières,
	Piloter financièrement l'activité d'une entreprise en s'appuyant sur des outils de suivi financier (dashboards, outils de BI[1] etc.) afin de garantir la viabilité de l'entreprise.		

[1] Business Intelligence

			ainsi que les impacts profit et trésorerie en utilisant les outils de dashboard ou de BI.

Ecole 2600

Identification des blocs de compétences de la certification

Intitulé :	Descriptif et modalités d'évaluation et de certification
Bloc 1 : Conseiller son entreprise en sécurité des systèmes d'informations.	Analyser les pratiques professionnelles des collaborateurs afin de proposer des améliorations dans leur application des normes, des standards et du respect du droit relatifs à la sécurité informatique dans les architectures de SI, ou les applications. Rédiger pour son organisation des notes, des guides, des présentations et/ou des directives d'application afin de réduire le risque en cybersécurité, qui s'appuient sur les éléments identifiés en phase d'analyse. Conseiller son organisation sur l'utilisation et sur la portée stratégique des notes, guides, directives d'application rédigées après l'analyse. Analyser son organisation afin d'augmenter la cyber résilience de celle-ci, en étudiant les éléments suivants: - Les menaces en cybersécurité relatives à l'activité de l'entreprise; - Le plan de continuité d'activité relatif aux crises cyber sécurités (PCA);

	- Le plan de reprise d'activité relatif aux crises cyber sécurités (PRA). Rédiger des notes, des guides, des présentations afin d'éclairer sa hiérarchie et d'augmenter la cyber résilience, qui s'appuient sur les éléments identifiés en phase d'analyse de l'activité. Défendre auprès de sa hiérarchie une vision stratégique en cybersécurité afin de prévenir le risque cyber sur le temps long. <u>Evaluation</u> : Exercices pratiques qui portent sur la conception, puis la rédaction des documents permettant de structurer l'organisation de la sécurité des SI en articulant un aspect sécurité (norme, standard, droit, ...) à la réalité de terrain de l'entreprise). Les documents sont ensuite défendus devant un jury. Mise en situation au travers d'étude de cas typique d'entreprise au choix (OIV, PMI, TPE, Grand groupe, ...) nécessitant la rédaction d'un PCA (Plan de continuité d'activité) cyber et d'un PRA (Plan de reprise d'activité) cyber soutenu devant jury. Mise en situation au travers d'étude de cas sur les stratégies cybers déployables dans des contextes précis et relatives à un type d'entreprise au choix (OIV, PMI,

	TPE, Grand groupe, ...). Les stratégies déployées sont soutenues devant jury.

Bloc 2 : Évaluer techniquement la sécurité de l'entreprise.	Évaluer les solutions d'analyse de menace et de contre-mesure de type COTS (Component On The Shelf), OSINT (Open Source Intelligence), ou autre applicable sur le SI de l'organisation afin de juger des opportunités d'amélioration de la sécurité des données, des systèmes et du réseaux. Analyser les évolutions technologiques en cybersécurité (techniques d'attaque et de défense logiciels, matériels ou sociales) afin de maintenir son niveau d'expertise dans le domaine et d'identifier de "nouveaux" risques potentiels. Participer aux innovations de la sécurité des SI publiés officiellement sur les canaux spécialisés (conférence, podcast, blog, ...) afin d'augmenter son expertise sur les potentiels risques pour le SI de l'organisation et mieux identifier de nouvelles attaques cyber. Contrôler la bonne application des notes, recommandations, guides et/ou des directives d'application rédigées/exprimées pendant l'activité de conseil concernant: - La conception et le développement sécurisé d'applications lourdes, web ou embarquées. - En conception et mise en œuvre d'architecture sécurisée de système d'information sur le SI de l'organisation Analyser les écarts entre les recommandations rédigées/exprimées pendant l'activité de conseil et la mise en œuvre technique afin d'établir des points de contrôle en

	utilisant les techniques d'attaques informatiques et les outils associés. Evaluation : Exercices pratiques qui portent sur la mise en œuvre des techniques d'attaque/défense ou d'outils spécialisés sur une infrastructure de simulation et de correction automatique suivie de l'écriture de compte rendu technique. Exercices pratiques qui portent sur l'investigation technique d'un projet informatique (SI, application, …) afin de contrôler la présence ou l'absence de faille exploitable à des fins malveillantes soit manuellement, soit par des outils. Mise en situation au travers de projets d'actualité de la cybersécurité afin de juger sa proactivité face à celle-ci. Cette mise en situation fait l'objet d'un rapport écrit expliquant et justifiant les choix de l'innovation apportée et sera soutenue oralement devant jury. Mise en situation au travers d'étude de cas nécessitant la réalisation d'un Audit sécurité soutenus devant un jury.

Bloc 3: Concevoir des solutions techniques sécurisées.	Concevoir l'architecture SI de l'entreprise dans le contexte d'un réseau informatique, télécom ou industriel afin de répondre au besoin fonctionnel de l'organisation en prenant en compte le plan de routage, le cloud, la localisation des services, le besoin exprimé de fonctionnalité du SI. Mettre en œuvre l'architecture SI de l'entreprise dans le contexte d'un réseau informatique, télécom ou industriel afin de rendre opérationnelles les nouvelles fonctionnalités en prenant en compte les solutions logicielles de déploiement d'architecture (ansible, puppet, ...) et les spécificités des systèmes visées (windows, linux, ...). Concevoir des solutions logicielles de façon sécurisée dans les contextes d'une application lourde, du web ou de l'embarqué afin de répondre aux besoins fonctionnels du produit visé en fonction des problématiques algorithmique, de performance, de l'architecture du code, et les interactions avec les bases de données. Mettre en œuvre les solutions logicielles de façon sécurisée dans les contextes d'une application lourde, du web ou de l'embarqué afin de rendre opérationnelles les nouvelles fonctionnalités en prenant en compte les spécificités des langages employés, des bibliothèques de fonctions, et des API de services tiers. Evaluation :

	Exercices pratiques qui portent sur la conception et la mise en œuvre d'un projet informatique (SI, application, ...) respectant l'application des bonnes pratiques en sécurité informatique. Mise en situation au travers de projets informatiques complets et concrets respectant toutes les consignes de production sécurisée: - Infrastructure SI partiel ou complète - Applications (standard, web, embarquée, ...) d'une entreprise répondant à une expression de besoin. Cette mise en situation fait l'objet d'un rapport écrit expliquant et justifiant les choix de la solution apportée (en intégrant la composante sécurité) et sera soutenue oralement devant jury.

Bloc 4 : Gérer une crise cyber	Evaluer les équipes techniques afin de réduire le risque en cybersécurité sur leur compréhension et leur application des notes, recommandations, guides et/ou des directives d'application rédigées/exprimés pendant l'activité d'audit Piloter les équipes techniques en situation de crise de cybersécurité afin d'apporter, par son expertise, la capacité de réagir rapidement et de s'adapter aux imprévus non couverts par les documents préventifs préalablement établis (PCA,PRA, autres...) Contrôler l'application des consignes de sécurité émises en phase conseil et lors de retour d'expérience à destination des équipes techniques afin de se préparer à une crise cyber. Analyser, en situation de crise de cybersécurité, les écarts entre les documents préventifs préalablement établis (PCA, PRA, autres...) et les incidents rencontrés afin d'alimenter le retour d'expérience. Rédiger un retour d'expérience sur les incidents rencontrés en crise cyber afin de maintenir et faire évoluer tous les documents préventifs préalablement établie (PCA, PRA, autres...). <u>Evaluation</u> : Exercices pratiques en groupe sur le management humain, la prise de décision, le développement des "soft-skills" via des jeux de rôle.

	Mise en situation au travers d'étude de cas portant sur l'analyse de PCA (Plan de continuité d'activité) cyber et de PRA (Plan de reprise d'activité) cyber sur lequel il faut identifier les points de contrôles dans l'organisation, planifier les missions des équipes techniques pour la mise en conformité , synthétiser le tout dans un rapport soutenus devant un jury. Mise en situation au travers de projets informatiques de groupe complets et concrets respectant toutes les consignes de production sécurisée: - Infrastructure SI partiel ou complète - Applications (standard, web, embarquée, ...) d'une entreprise répondant à une expression de besoin. Mise en situation au travers de compétitions en équipe de sécurité chronométrées de type CTF (Capture the Flags) Jeopardy et/ou en Red/Blue team (attaque/défense) suivie de l'écriture de compte rendu technique et situationnel sur le déroulement du concours. Mise en situation au travers de scénario de crise (type red/blue team), de cas typique d'entreprise au choix (OIV, PMI, TPE, Grand groupe) nécessitant la mise en application d'un PCA (Plan de continuité d'activité) cyber puis d'un PRA (Plan de reprise d'activité) cyber. Suivie de l'écriture de compte rendu technique et situationnel sur le déroulement de la crise soutenu devant jury.

Bloc 5: Entreprendre dans le secteur cyber.	Analyser l'écosystème cyber via une étude de marché afin d'identifier des opportunités de création d'entreprise. Concevoir un lean canevas et business plan prenant en compte les éléments financiers prévisionnels, les opportunités du marché, les éléments commerciaux et marketing afin de convaincre de la solidité du projet auprès des futurs investisseurs. Définir une stratégie d'investissement conforme avec le business plan en prenant en compte la valorisation du projet et le cycle de financement (amorçage, dispositifs de BPI France, fonds d'investissements) afin de convaincre des partenaires de financer le projet. Définir une stratégie marketing et commerciale pour adresser les clients potentiels grâce à des canaux de distribution, une stratégie de prix compétitif et à un CRM performant en accord avec le business plan. Piloter financièrement l'activité d'une entreprise en s'appuyant sur des outils de suivi financier (dashboards, outils de BI etc.) afin de garantir la viabilité de l'entreprise. <u>Evaluation :</u> L'analyse de marché proposée identifie les éléments business et technologiques de la concurrence. Le Business Plan répond aux dix critères d'évaluation suivants: rentabilité, adéquation homme/projet, adéquation produit/marché,

	innovation, faisabilité technique, création d'emploi, cohérence, pertinence, pérennité, apport personnel. Le Lean Canevas reprend le problème, la solution, l'indicateur de performance, la proposition unique de valeur, l'avantage compétitif, les Canaux, les segments de clientèle, les coûts et les sources de revenus. La présentation investisseur identifie la raison d'être, le problème adressé, la solution, le pourquoi maintenant, la taille de marché, le produit, l'équipe, le modèle économique, la compétition et la projection financière La stratégie marketing et commerciale identifie les canaux d'acquisitions (growth marketing, acquisition payante etc.), l'argumentaire de vente, le traitement des objections ainsi que les outils nécessaires à mettre en place (CRM, outils marketing…) Au regard des exercices sur les activités courantes de gestion, les candidats sont évalués sur leur capacité à relier les éléments opérationnels et leurs conséquences financières, ainsi que les impacts profit et trésorerie en utilisant les outils de dashboard ou de BI.

Rappel sur les étudiants en situation de handicap

Pour rappel, concernant les étudiants en situation de handicap, l'École 2600 souhaite adapter son processus de recrutement ainsi que le déroulé de la scolarité pour tenir compte de leurs besoins spécifiques.

Nous avons souhaité faire en sorte que les lieux d'études (cours et bootcamp), le système d'enseignement à distance ainsi que les modalités de suivi pédagogique soient totalement adaptés aux personnes en situation de handicap.

Pour cela, nous avons porté un soin attentif à l'infrastructure de l'École est aux normes ERP, notamment pour nos futurs étudiants ayant des problèmes de mobilité.

Concernant les cours, nous avons opté aussi pour des aménagements matériels spécifiques:

- assises confortables
- secrétaire d'examens
- soutien pédagogique
- tutorat d'intégration

ainsi que des aménagements organisationnels:

- aménagements des emplois du temps
- aménagement de cursus
- aménagement des examens (exemple: 25 % de temps supplémentaire)

Concernant les examens, tout étudiant en situation de handicap ou présentant une maladie invalidante a le droit de bénéficier d'aménagements pour ses études ou ses examens. Pour évaluer vos besoins en compensations, l'École 2600 dispose d'un référent handicap afin de l'assister.

Nous souhaitons contribuer à cette forme d'inclusion, sachant que notre secteur peut s'avérer un réel lieu d'épanouissement professionnel et personnel.