Valnaos
IT Training & Consulting

Professional Cloud Security Manager

Référence en action collective fafiec : gouvernance et sécurité - module socle

La formation Professional Cloud Security Manager PCS de CCC (Cloud Credential Council) vous permet d'explorer les concepts liés à la sécurité, au risque et à la mise en conformité dans un environnement Cloud. Vous comprendrez les risques et l'impact du Cloud Computing dans le business et les défis techniques de sécurité. Le formateur est certifié pour délivrer la formation.

Objectifs

- Appliquer les meilleures pratiques de règles de gouvernance et de sécurité
- Expliquer ce qui sécurise les différents services Cloud et les modèles de déploiement
- Expliquer le design sécurité au regard de l'infrastructure, des configurations et des applications
- Comprendre, appliquer et analyser comment gérer l'accès aux ressources Coud, des méthodes pour sécuriser les data, operating systèmes, les applications, l'infrastructure Cloud
- Passer dans les conditions optimales la certification internationale «Professional Cloud Security Manager»

Prérequis

- Des connaissances en langue anglaise et il est souhaitable d'avoir 5 ans d'expérience dans la sécurité des entreprises et une bonne compréhension des services du Cloud Computing et des modèles de déploiement. Il est conseillé d'avoir suivi et d'être certifié Cloud Technology Associate (connaissances du cloud – module socle)
- Se munir de sa pièce d'identité pour le passage de l'examen

Public

- CDO (Chief Digital Office), professionnels Sécurité IT, professionnels du risque et de la conformité, Auditeur des services Cloud Computing, Administrateur/Ingénieur réseau, consultants et opérationnels IT.

Durée :

- 3 journées : 9h00-17h00 - 21 heures (Travail personnel non inclus)
- Intégrant 1 pause matin et après-midi et pauses déjeuners

Déroulement pédagogique

Projection du cours. La formation est en langue française, le support et l'examen sont en langue anglaise. Le cours est théorique à 60% et 40% pratique avec des discussions, partage d'expérience et étude de cas. Préparation à l'examen avec des examens QCM à blanc. Une attestation de formation est délivrée en fin de formation.

Déroulement de l'examen

- QCM de 25 questions avec scénario en langue anglaise (les candidats peuvent amener un dictionnaire format papier)
- Obtention du diplôme à partir de 65%
- Durée : maximum 75 minutes + 15' pour les non anglophones

Programme

Sécurité, risques et gouvernance : les concepts, la gestion de la sécurité IT, la gouvernance IT, la sécurité du Cloud Computing. Implémentation des traitements et mitigations de risque Cloud, les impacts business et techniques sur la politique de gouvernance.
Les menaces de sécurité et les défis : différence de gouvernance traditionnelle et Cloud, les différences entre la sécurité partagée et le modèle de conformité dans le Cloud – les risques et les impacts en termes business et technique et leurs conséquences sur la politique de gouvernance technique : protection/classification des data, modèles de menaces, ISA – SLA - Asset partagés
G**estion de Sécurité dans le Cloud** : la classification des données et son importance- les risques et les mesures pour réduire les menaces de sécurité. La confidentialité et la gestion/implémentation des identités (IAM). Les problématiques d'accès, de confidentialité, de risque et de conformité. Les modèles de services et de déploiement qui impactent la valeur business.
Légal, contractuel et monitoring opérationnel dans le Cloud : concepts- les défis -implémentation des mitigations liées aux éléments clés légaux – risques et opportunités des services monitorés cloud.
Gestion du réseau de sécurité dans le Cloud : la gestion de la vulnérabilité et l'architecture sécurité au regard du Cloud et de son rôle - SDN – NVS - les avantages de la virtualisation, la gestion Patch et les tests de pénétration.
Continuité du business, restauration de désastre et planning de performance et de capacité : concepts de la continuité business (BC) et de la restauration du désastre (DR), les défis, l'implémentation de la capacité dans le BC et DR, les risques et opportunités, le concept de la planification de la Capacité et de la Performance.
Pratiques de gestion de sécurité cloud avancée : spécificité sur les enjeux de la gouvernance et de la sécurité sur un modèle PaaS – pise de conscience des enjeux de sécurité et de gouvernance pour concevoir et gérer les systèmes PaaS. Développement standard – sécurité API.
Planning de sécurité, standards et évolution du cloud : process de sécurité et enjeux des software, application et services opérées dans le cloud – planning – contrôle et audit et évolution de la sécurité du cloud
Révisions et passage de l'examen final en fin de formation (voir le déroulement de l'examen)