IDB2937 - Spécialiste principal de la gestion des identités et des accès

Postuler à ce poste

Unité commerciale :	Directeur général Services corporatifs
Division:	N'est pas applicable
Département:	Gestion de l'information et technologies perturbatrices
De campagne:	Arabie Saoudite
Lieu:	Arabie Saoudite - Djeddah
Date de clôture:	14-janv-2023

Département:

Gestion de l'information et technologies perturbatrices

Objectif:

Le spécialiste principal de la gestion des identités et des accès est chargé de concevoir, de mettre en œuvre et d'exploiter le programme de gestion des identités et des accès, y compris les processus, les normes et les solutions pour toutes les applications informatiques, les services informatiques et les composants des technologies de l'information, afin de gérer la manière dont les utilisateurs professionnels et le personnel informatique accèdent aux données et afin de réduire le risque d'accès non autorisé et de garantir que des contrôles préventifs, de surveillance et réactifs adéquats pour la gouvernance, les risques et la conformité sont établis pour gérer le risque résiduel dans le cadre de l'appétence au risque de l'organisation. Le spécialiste principal de la gestion des identités et des accès effectue à la fois la surveillance stratégique et la gestion quotidienne des tiers pour s'assurer que les services de gestion des identités et des accès répondent aux besoins organisationnels.

Principales responsabilités:

- Concevoir et maintenir l'architecture et la feuille de route de gestion des identités et des accès en collaboration avec les architectes d'entreprise, les architectes de solutions, les opérations de solutions et les opérations d'infrastructure à travers le paysage technologique des applications et de l'infrastructure informatique pour gérer l'authentification et l'accès à tous les systèmes et données IsDB
- Collaborer avec les fonctions d'architecture d'entreprise, de risque technologique, de gestion des risques et d'audit interne pour répondre aux exigences complexes de gestion des identités et des accès dans le cadre du modèle organisationnel des trois lignes de défense

- Élaborer et maintenir des politiques, des processus et des procédures de gestion des identités et des accès conformément aux cadres et aux normes de l'industrie en coordination avec la fonction Technology Risk and Assurance
- Assurer la conformité aux politiques, normes et directives organisationnelles de gestion des identités et des accès pour le siège social et les hubs régionaux couvrant les services cloud, les centres de données, le réseau, les serveurs, les solutions de communication, les sites de reprise après sinistre, l'informatique de l'utilisateur final, les bases de données, les plates-formes de solutions, les applications commerciales et les sites Web
- Gérer les tiers fournissant des opérations de gestion des identités et des accès pour le siège et les hubs régionaux afin de garantir un accès approprié pour les utilisateurs professionnels et le personnel informatique du paysage informatique conformément aux politiques, processus et SLA définis
- Collaborer avec les équipes de livraison de solutions et d'opérations technologiques pour intégrer de nouvelles applications d'entreprise et de nouveaux services informatiques aux solutions et processus de gestion des identités et des accès dans le cadre de la transition des solutions d'entreprise et des services informatiques de la phase de mise en œuvre à la phase d'exploitation
- Participer en tant que membre permanent du comité consultatif sur les changements pour s'assurer que tous les changements au sein de l'environnement technologique de la BID sont conformes aux politiques et normes de gestion des identités et des accès
- Planifier et gérer la mise en œuvre d'évaluations proactives des risques et d'examens de conformité pour évaluer les risques associés à l'accès aux systèmes et aux données de la BIsD et surveiller la conformité aux normes et processus d'accès dans l'environnement informatique de la BIsD
- Veiller à ce que les politiques, les processus et les normes du cycle de vie de l'identité couvrant les scénarios de recrutement, de transfert et de départ soient définis et adoptés pour toutes les catégories d'utilisateurs qui ont besoin d'accéder au système et aux données de la BID, y compris le personnel, les consultants, les sous-traitants et autres
- Diriger la planification et la mise en œuvre d'examens d'accès périodiques dans les solutions d'entreprise et les composants de l'infrastructure informatique pour garantir un accès approprié aux systèmes et aux données pour les utilisateurs professionnels, le personnel informatique et les tiers afin de réduire le risque d'abus ou de fraude
- Établir et maintenir des normes techniques pour la conception et la mise en œuvre de l'authentification et de l'autorisation pour toutes les applications, services informatiques et composants technologiques de la BID
- Concevoir et mettre en œuvre des normes, des processus et des solutions pour gérer et surveiller l'accès privilégié aux systèmes et aux données de la BID afin de réduire le risque élevé lié à l'accès des super utilisateurs au sein de l'environnement informatique
- Superviser les deuxième et troisième niveaux de support et de réponse aux incidents et demandes d'identité et d'accès
- Gérer la mise en œuvre et l'intégration de la surveillance des identités et des accès dans l'environnement informatique de la BIsD dans le cadre global de surveillance de la sécurité
- Concevoir et mettre en œuvre l'intégration des processus et des solutions de gestion des identités et des accès avec les processus et les solutions de gestion des services informatiques, y compris l'intégration de la portée et des processus couverts par les fournisseurs de services tiers
- Gérer le paysage de solutions qui prend en charge les processus de gestion des identités et des accès, y compris l'authentification, la gouvernance des identités, l'administration des identités, la gestion des identités privilégiées et la conformité
- Fournir une formation et une sensibilisation sur les sujets de gestion des identités et des accès dans les solutions d'entreprise et les services informatiques pour améliorer l'adoption lors de la mise en œuvre de la solution, des opérations d'infrastructure et de sécurité, de la gestion des services informatiques et d'autres domaines conformément aux politiques, processus et normes organisationnels
- Préparer et présenter des rapports détaillés et récapitulatifs sur la gestion de l'accès aux identités pour représenter avec précision les plans, l'état et les risques pour IMDT, les entreprises et les parties prenantes de la direction

Conditions:

Qualifications académiques et professionnelles :

- Baccalauréat en informatique, en génie, en technologie de l'information ou dans un domaine connexe

De l'expérience:

- Plus de 8 ans d'expérience en sécurité de l'information et en gestion des identités et des accès

Langues :

- Anglais - Obligatoire
- Arabe - préféré
- Français - préféré

Compétences et connaissances nécessaires :

- Expérience dans l'architecture, la conception et la mise en œuvre de solutions de gestion des identités et des accès, y compris pour les accès privilégiés
- Expérience dans la gestion des opérations de gestion des identités et des accès
- Expérience dans la conception de normes d'authentification et d'autorisation

- Expérience dans la conception et la mise en œuvre de processus de recrutement, de déménagement et de départ
- Expérience dans la planification et la réalisation d'examens d'accès, d'évaluations des risques liés à l'accès et d'examens de conformité aux normes liées à l'accès
- CISSP, ISO 27001, CISM ou autre certification reconnue par le secteur de la sécurité de l'information
- Bonne compréhension des exigences d'intégration pour les solutions d'affaires et les composants de l'infrastructure informatique pour la gestion des identités et des accès

Postuler à ce poste

< Retour à la recherche

Connecte-toi avec nous