

Identity Access Management Analyst

Référence : 2021-01193

CDI TUNIS IT

- Offre à la Une :
- Localisation : TUNIS
- Type de contrat : CDI
- Date de première publication : 19/08/2021
- Domaine d'activité : IT
- Lieu du poste : Les berges du lac 2

Activité

ODDO BHF Tunis is a growing financial services company created in 2009 to support the development of the ODDO BHF Group.

With more than 280 employees, it now operates in two main areas: financial analysis and IT.

The equity research team contributes to the coverage of more than 400 listed European companies and the success of the ODDO Securities research department, which enjoys a strong international reputation.

The IT team ensures the development of all websites and provides its expertise to the Group's major IT projects.

Innovative in the Tunisian market, ODDO BHF Tunis is developing rapidly and aims to double its workforce as part of the Group's development.

Descriptif du poste

Job Description

The Identity and Access Management (IAM) team is responsible for managing the identity and application access life cycle for users inside the organization and ensures each user has the correct attributes and entitlements across diverse services/applications. The team is also responsible for day-to-day operations of the IAM team. The team ensures that projects; incidents and service requests are completed on time and within scope.

The candidate will be a team player working to expand the integration of our identity management solutions with our enterprise applications, support day-to-day requests like writing scripts for reports requested from the business, troubleshooting and operations of our Identity Management environment. In addition to having strong technical skills, you must be comfortable in effectively communicating with business end-users, technical IT teams and business partners, all while being sensitive to a wide diversity of cultural and technical backgrounds in a global business environment.

Responsibilities

Provide Level 3 Functional Support to users for the Identity and Access Management Platform (Level 1: Helpdesk, Level 2: User Access Management of target applications) via request management tools and functional mailboxes**.**

Troubleshoot and manage the resolution of issues related to identity static data, access static data (like functional descriptions, flagging of parameters, accounts, entitlements etc).

data quality assurance and data issue remediation by updating actions (HR imports, various scripts, remediation projects) carried out in close collaboration with 1st line of defense (IT Governance) and 2nd line of defense (Information Security Management)

Onboard in-house applications and third-party applications to the IAM system for identity and access provisioning.

Ensure that the maintenance, operating, and monitoring of IAM system is in place and completed on schedule.

Work to ensure audit tasks related to Identity Management are completed on time, with participation of relevant stakeholders.

Complete the key metric reporting and analysis for the Identity Management environment as required.

Utilize industry best practices for appropriate standards, processes, procedures, tools and documentation.

Profil et compétences recherchées

Bachelor's Degree in Information Systems or related field.

Working knowledge of Microsoft SQL.

Experience configuring and managing IT systems with technologies such as VB.NET, XML, SOAP, JSON/REST, SQL, Windows, and databases.

Adept at PowerShell & VB scripting, VBA, Excel, regular expressions, policy management, etc.

Customer service driven/focused with a proactive and positive can-do approach. Demonstrates commitment to the organization’s policy framework and practices continuous improvement.

Demonstrate ability to prioritize and multi-task.

Demonstrate effective problem-solving, analytical, and time management skills.

Ability for troubleshooting and problem analysis is required, along with the ability to clearly communicate the results of problem analysis to business stakeholders, IT support teams to quickly and effectively resolve operational issues.

Experience in troubleshooting, managing and solving issues related to identities, systems, access, accounts, authentication, authorization, entitlements, and permissions

Demonstrated organizational skills, attention to detail and ability to work both independently and as part of a team.

Good written, oral, and interpersonal communications skills.

Technical skills or experience in the Identity Access Management (IAM) space is a plus.

Experience in Identity and Access Management (IAM) concepts and associated technologies is a plus.

Knowledge of IAM software such as One Identity Management is a plus.

Prove ability to work with diverse groups of individuals and work effectively with all staff.

International experience beneficial; multiple language skills (French, English, German is a plus)