**Please describe your knowledge of IdAM tools and techniques, including Oracle IDCS, SAML, LDAP**

We have extensive knowledge of IDAM and IDAM tools both native and 3rd party. We design, build and manage cloud environments for a variety of customers in the public/private sector and branches of the military.

IDCS is Oracle’s own Identity as a service (IdaaS) tool set. It has been proven to be a seamless integrator with On-Premise Active Directory to provide single sign-on between Cloud and On-Premise applications. Through its Identity Bridge component IDCS can synchronise all the identities and groups from Active Directory into its own ID Store. For Oracle on-prem to OCI this is the IDAM tool of choice.

SAML is also widely used on a number of our customers. SAML is designed for cloud-based connections using only an IdP and SP to communicate user data. So it won't be the IDAM of choice initially here but once migrations have been completed and everything is cloud based we would look to leverage it. We have a core cyber security and identity management team responsible for these activities in both delivery and operational functions.

LDAP is the most widely used authentication method and we have an engineering team of more than 20 dedicated people, responsible for design, build and maintenance of solutions using it. Customers using it are a wide spectrum of public/private sector, financial services, banking etc, all of whom are subject to rigorous compliance standards. This is also the authentication choice for migration projects where a physical infrastructure is in use.

Our standard approach to Identity and Access Management (IdAM) tools and techniques, such as Oracle Identity Cloud Service (IDCS), SAML (Security Assertion Markup Language), and LDAP (Lightweight Directory Access Protocol), include consideration of the following:

1. Single Sign-On (SSO)
2. Enterprise Authentication and Authorization
3. Federation considerations and integration
4. Web Application Security
5. Cloud Services Integration
6. API Security
7. Directory Services
8. Access Control and Role-Based Access Control (RBAC)
9. Multi-Factor Authentication (MFA)
10. Self-Service Password Reset and User Profile Management
11. Mobile Device Management (MDM)
12. Compliance and Audit
13. On-Premises Integration

These tools and techniques can be used in combination or separately, depending on your organisation's specific needs and the complexity of your identity and access management requirements. They play a crucial role in enhancing security, user experience, and compliance within your IT ecosystem.

Single Sign on is a core requirement when implementing a new application as it helps improve user experience as well as addressing core security requirements. As part of our delivered Finance Transformation programmes enabled by Oracle Cloud, PwC have set up single sign on at multiple clients to connect to Oracle Cloud applications (both SaaS and PaaS) without users being promoted for their sign-on credentials twice. In a majority of implementations, the Azure AD has acted as the Identity Provider (either Cloud or on-Prem), with the Oracle applications being the Service provider. This minimises the need to significantly change the existing IdP architecture. Recently client implementations include Direct Line Group and MS Amlin.

The Cloud Managed Services (CMS) team, within PwC, provide services that meet or exceed the standards and requirements of the external accreditations detailed below and ensure these are maintained

* ISO 27001 - Security
* ISO 20000 - Service
* Cyber Essentials Plus
* ISO 27701 - Info Protection
* ISO 9001 - Quality