

Security in the Cloud

The growing number of cloud computing services promise appealing cost-savings and flexibility. Yet cloud computing may seem risky because you cannot secure its perimeter – where are a cloud's boundaries? How do you ensure the security of data hosted in cloud data centres?

Whether you host information and services in data centres that are on your premises or in the cloud, the same security principles apply. You must look carefully at how well cloud providers protect key functions and sensitive data and tailor your security tactics to the services you use, whether that service is software, databases, storage or platforms.

Customers expect their data and applications stored in the cloud to remain private and secure. While the challenges of providing security and privacy are evolving along with the cloud, the underlying principles haven't changed.

Supporting any organisation's journey to cloud computing requires an honest assessment of an organisation's readiness to conduct cloud-based Identity and Access Management (IAM), as well as understanding the capabilities of the organisation's cloud computing providers.

Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today. Extending an organisation's identity and access management strategy into the cloud is a necessary prerequisite for strategic use of on-demand computing services.

These are the identity and access management functions that are essential to the successful and effective management of identities in the cloud:

- **Identity provisioning:** One of the major challenges for organisations adopting cloud computing services is the secure and timely management of on-boarding (provisioning) and off-boarding (deprovisioning) of users in the cloud. Enterprises that have invested in user management processes within will seek to extend those processes to cloud services.
- **Authentication:** When organisations utilise cloud services, authenticating users in a trustworthy and manageable manner is a vital requirement. Organisations must address authentication-related challenges such as credential management, strong authentication, delegated authentication, and managing trust across all types of cloud services.
- **Federation:** In the cloud computing environment, Federated Identity Management plays a vital role in enabling organisations to authenticate their users of cloud services using the organisation's chosen identity provider. Organisations considering federated identity management in the cloud should understand the various challenges and possible solutions to address those challenges with respect to identity lifecycle management, available authentication methods to protect confidentiality, and integrity, while supporting non-repudiation.
- **Authorisation and User Profile Management:** The requirements for user profiles and access control policy vary, depending on whether the user is acting on their own behalf (such as a consumer) or as a member of an organisation (such as an employer, university, hospital, or other enterprise). The access control requirements in service provider identity environments include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way.
- **Compliance:** For customers who rely on cloud services, it is important to understand how Identity Management can enable compliance with internal or regulatory requirements. Well designed identity management can ensure that information about accounts, access grants, and segregation of duty enforcement at cloud providers, can all be pulled together to satisfy an enterprise's audit and compliance reporting requirements.

For more information and to request a consultation from Sysec on secure identity and access management in the cloud please contact info@sysec.co.uk