# Identity and Access Functions

Identity and access management (IAM) is the cornerstone of cybersecurity and plays a huge role in other IT management processes. BigU’s IAM processes facilitate Single Sign On (SSO) using three tools: Microsoft’s Active directory, an identity governance and administration (IGA) system, and dual authentication services. Some credentials do exist outside of that environment for specialized purposes, particularly for some IT management processes, but these tools and the related oversight processes largely harmonize identity and access functions.

**User Access to Devices and Productivity Tools**

As in any digitized organization, phishing-related risks where a user introduces vulnerability in a network or system through credential compromise or installation of malware are a huge threat to BigU’s operations. BigU primarily Microsoft 365 tools for email, word processing, spreadsheets, and other productivity applications. But, as would be expected in a University setting, tools from Google, Box, and other familiar vendors are supported. BigU uses a Learning Management System that needs to integrate various services, including role-based access and identity services. “Connectors” between active directory and other systems are needed for BigU to fulfill its mission.

**Access to ERP Services**

This cloud directory service is connected to the ERP system allowing application-level authorizations to be supported by platform level authentication and threat detection tools. However, as is typical for this kind of deployment, administrative functions for managing the cloud services and some other infrastructure elements are not. There are great reasons for this. Consider, for example, what might happen if the connection between the IGA tools and the cloud provider configuration were disrupted. BigU people would not be able to log into the services to fix the problem. Similarly, administrative access to routers, VPN gateways, firewalls, and other network gear might be cut off, leaving service down if access to centralized IAM tools were to be disrupted.

An IT auditor would want to look into the mechanisms associated with these privileged activities. On the one hand, compromise of accounts with administrative control over IGA, cloud service, or network components could be devastatingly impactful as nearly all other security controls could be disabled. But on the other hand, centralized control over the IAM functions for these resources needs to have some independence from regular operations. This tension is a reality for most every significant IT system.

BigU has a variety of controls in place to protect against related risks. The cloud service provider manages accounts for users authorized to reconfigure cloud services. The provider’s IAM practices are tightly controlled, intensely monitored, and systematically audited. BigU could create big problems for itself it was careless about how such accounts are provisioned, deprovisioned, or managed, but the cloud provider has established strong practices internally and provides solid guidance for its clients to protect privileged access.

At the application level – that is for security and configuration activities related to the ERP – the cloud infrastructure limits access to administrative consoles to devices coming from identified segments of the BigU network. That means that, in addition to the already strong application controls over authentication and authorization, an outside actor would have to penetrate a carefully protected BigU network segment (or access gateway) before it could even pass web access requests to the ERP configuration console.

The big picture here is that IAM in the cloud is subject to familiar risks. But by placing the services in the cloud, BigU has exposed its systems to access requests from anywhere in the world through networks that are not directly under its control. Many would say that the controls in the cloud are stronger than what an organization can provide locally. Fair enough. Still, the cloud environment calls for different control activities. Auditors need to gain an understanding of the identity infrastructure if they are to provide reasonable assurance.