Given the projected hurricane that is expected to implode colossal damage onto us. The insurance team can readily deploy virtual machines to decrease the load of work from the natural disaster. But that will require security tightening between enterprise system and virtual machines. Therefore this introduces us to RBAC. “Role-based access control (RBAC) restricts network access based on a person's role within an organization and has become one of the main methods for advanced access control.” (Ellen Zhang of Digital Guardian). RBAC uses roles to manage rights and permissions for users. This control is effective for a specific department looking to perform the same job functions. Which in turn gives us the ability to say who has access, how much, and what type of access. An important consideration with using cloud service models is the difference in responsibilities assigned to a Cloud Service Provider(CSP). In this setting, we will be using Microsoft Azure as our primary CSP. When picking Azure as our focus, the insurance organization must scrutinize various security control features which include Roles, Secure Remote Access, Policies, Encryption, Federation Single-Sign On(SSO), Logging and Monitoring, and Resources Permissions.

A role is an assembly collection of permissions granted to us by the administrator. Allowing us a list of actions we can potentially perform when admitted. Such as reading, writing, editing, or perhaps deleting. In the Azure functionality, a role assignment consists of three elements: security principal, role definition, and scope. The security principal is security identification to access specific Azure resources. Azure also has built-in roles that can we also used. Virtual Machine Contributor allows the user to create the virtual machine and handle the necessary actions. While Scoping is allowing a specific action to be tailored to that group or role once assigned.

Cloud security is about maintaining that balance of allowing people access to what they need to get done but not compromising the security protocols. Which could bring too much risk, leaving the organization open to threats and attacks. By using Virtual Private Network(VPN) we can allow users to access private networks through public network. Though VPN have become a popular attack vector, enabling encryptions on the traffic for different tunnels will hugely protect the data from unauthorized disclosure.

By having a security policy in place, we can create certain conditions of authority and privileges. When enforcing the resources by the enterprise, there must be an understanding business leadership and roles written out. To systematize the policy, we will need to assign them through Azure portal, Powershell, or Azure CLI. the CSP resource policies ensure enterprise employees don't create more resources than their plan allows.

Encryption protects the confidentiality of data. Thankfully Azure provides prevailing encryption services. This prevents unauthorized personnel from accessing the data. “Microsoft Azure offers a variety of data storage solutions to meet different needs, including file, disk, blob, and table storage.” All are available across the service of SaaS, LaaS, and also PaaS.

Single Sign-On(SSO) refers to a user’s ability to log on once and access multiple systems without logging on again. SSO increases security because the user only needs to remember one set of credentials and is less likely to write them down. It’s much more convenient for enterprise to access network resources if they only have to log on once. “Azure Active Directory Seamless single sign-on (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames.”

Azure Monitor is a service in the Azure Cloud that helps you increase the performance and availability of your applications and services. By collecting and analyzing on cloud premise. Metrics are automatically collected when we start to use Azure resources. Logs are then collected that show the activity in the Azure subscription. All of these resources can be access through the Azure Portal. Working to monitor while access the features to help amass data collected across all of the applications and services.

“The Azure Storage platform is Microsoft's cloud storage solution for modern data storage scenarios. Azure Storage offers highly available, massively scalable, durable, and secure storage for a variety of data objects in the cloud.” the CSP Azure integrates security controls into the cloud-based resources which supports Resource Permission. Identifying who can access the data. While the processes differ with different CSP, the concept is similar to file system permission.

(n.d.). Retrieved from https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview.

Zhang, E., Lord, N., Zhang, E., & Brook, C. (2022, November 7). *What is role-based access control (RBAC)? examples, benefits, and more*. Digital Guardian. Retrieved February 8, 2023, from https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more