Case Study: SnowBe Online

SnowBe Online is a lifestyle brand for those who love the beach and snow. The owners started the company with a laid-back culture. Their customers instantly connected with their brand taking them to $100 million in sales in three years. After being so successful, the management team decided to take the company public.
Technical Overview:

1. The majority of their sales are processed online through their website, housed on the AWS platform.
    a. All credit cards are accepted and stored on the company's website database.
    b. All customer information and purchase history are stored on the website indefinitely.
2. They have multiple storefronts in the U.S. and Europe, which accept checks, cash, or credit cards. The credit card transactions are processed using bank-provided credit card terminals in each store.
3. There are twenty desktops and thirty laptops in the main office in Los Angeles.
    a. The desktops are used to run the business and customer support.
    b. The thirty laptops are used for sales (retail and wholesale). The laptops use a VPN to log into the office to access company applications.
4. There are six servers (on-premise and AWS) for access management, storage, customer relations management, order management, accounting, and vendor applications.

As a result of SnowBe's laid-back culture, they neglected to implement technical controls and processes. So, three months ago, Karen was assigned as the project manager to work on IT security. She recently hired Brad, an IT and cybersecurity consultant, to get their neglected systems and processes under control. Brad was initially hired to implement the following items:

1. To add an Active Directory (AD) server - A new server was added for AD. All users were added to AD and configured to access only the data they need to do their job. The process for adding new users and assigning permissions was documented to ensure all future users are similarly added.
2. To add a new firewall to the infrastructure. The configuration and settings for the device were documented for the team.
3. To add Anti-virus software to the infrastructure. The configuration and settings were documented for all desktops, laptops, and servers.

4. To add a new on-premise backup server to the infrastructure. All desktops, laptops, and servers were configured for backups. The configuration and settings were documented for the server.
5. Remote monitoring and management (RMM) software was added to all desktops, laptops, and servers (See "What is RMM" in the resources).   The configuration and settings were documented for all desktops, laptops, and servers.

Karen asked Brad about the next best steps to increase SnowBe's technical maturity without any financial commitment. Brad requested to start with an initial review of the IT environment. He decided to use the Simple Maturity Model Assessment Tool to quickly get an idea of security gaps, to gather the next best steps for SnowBe's technical maturity direction, and to be able to quote the work.