Cloud Services - Strategy And Risk

technology risk management pandemic

Summary: With the need to move work off-site, community financial institutions have likely turned to cloud service providers to help. We highlight some of the risks and the need for cloud strategy.

There are lots of different types of clouds: cumulus; stratus; stratocumulus; and nimbostratus, among others. But, the clouds getting all of the attention these days are cloud services.

It is a different time, to be sure. With businesses pushed to work remotely, cloud services have increased dramatically. In fact, Microsoft noticed a 775% increase in demand for its cloud services during the crisis. Like many businesses, community financial institutions (CFIs) may have turned to cloud service providers to streamline some of their workflow processes as they manage business off-site too.

Cloud Strategy. To start, it is important to have a cloud strategy. According to Accenture research, only 25% of banks have one of these, but this will become more vital with the ramp-up of more digital services. Most simply, this strategy should align with your business strategy and address the IT elements, including cybersecurity, for your continuing digital advancements. Now is the time to get this in place, if you haven't.

Cloud-Specific Risk. While cloud services played a role in keeping operations running during the coronavirus, the same risks (if not greater) need to be managed as before COVID-19. In response to these risks, the Federal Financial Institutions Examination Council (FFIEC) released a statement on risk management for cloud computing security at the end of April to remind bankers of the important practices to follow. This guidance is not new but was provided as a strong reminder as cloud services are in strong demand during this crisis. Here are the highlights:

- Implement suitable controls specifically for virtual infrastructure
- Set up specific security measures to address vulnerabilities present when using containers. Containers offer a packaging mechanism in which applications can be used outside of the environment in which they actually run, (i.e., Windows or Linux)
- Use managed security services, such as cloud access security broker (CASB) tools, which sit between cloud service users and cloud applications, to monitor all activity and enforce security policies
- Consider the interoperability and portability of data and services and how to appropriately scale security measures to address these capabilities
- Ensure suitable procedures are followed for the destruction and sanitation of your institution's data (and ensuring cloud vendors do the same)

Even after this crisis passes, remote and digital services will likely remain important for the banking industry. Digital banking has skyrocketed and is not expected to drop off after the coronavirus as many more people have become comfortable with it. According to FIS, new mobile banking registrations increased by 200% in April and mobile banking traffic jumped 85%. As business customers of CFIs become more tech-savvy and request newer features, CFIs may need to rely more heavily on cloud service providers.

Many CFIs were thrust into more cloud services due to the coronavirus. Now is the time to dot your i's and cross your t's, as things are starting to stabilize a bit, since the cloud is here to stay.

ON-DEMAND HELP FOR FINANCIAL INSTITUTIONS

Financial institutions face many difficult challenges, but you are not alone. Our experts stand ready to help you address a variety of issues. Find out more about our solutions today.