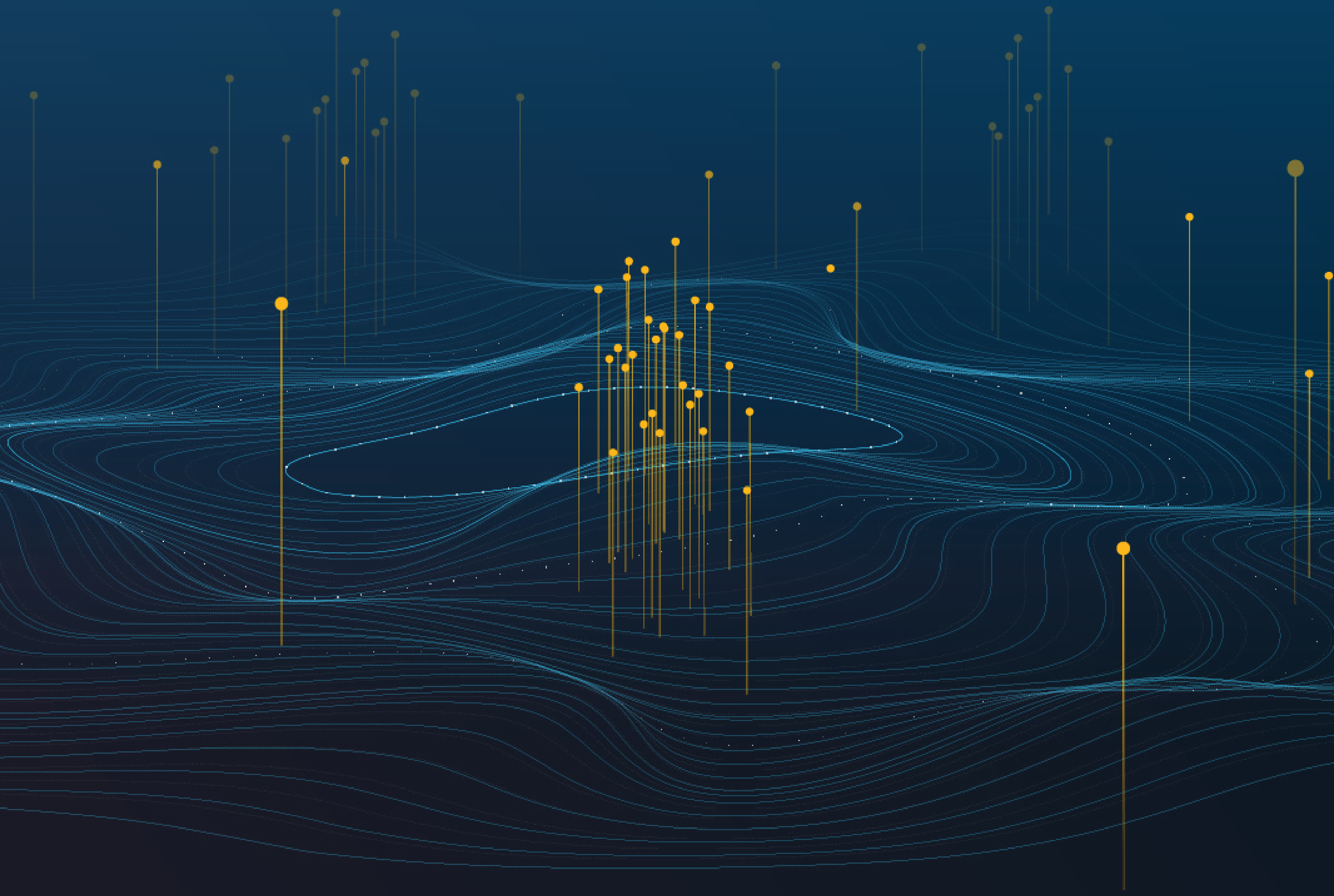
logicworks

Disaster Recovery for the Cloud Era



www.logicworks.com

Introduction

In today's modern data-driven cloud era, companies are managing more customer data than ever before with a growing need to recover quickly from IT disruptions. Data is used to innovate, improve products, and customize services for customers, enabling companies to gain and retain a competitive edge in the market.

Contrary to popular belief, the cloud is not foolproof. Establishing the right Disaster Recovery (DR) strategy for your cloud applications will enable you to quickly recover with minimal data loss when a failure inevitably happens. Common scenarios that can lead to service outages and data loss are malicious attacks, natural disasters, and human error.

In this eBook, we will unpack common DR strategies, provide clarity on Disaster Recovery versus high availability, and explore the potential business ramifications of a disaster.

High Availability is Not Disaster Recovery

It's often confusing to distinguish high availability from Disaster Recovery, and it's important to clearly identify their differences.

High availability can be defined as a system that aims to ensure an agreed level of operational performance, usually uptime, for a higher-than-normal period. It leverages redundancy in systems to overcome component failures, for example, running a website on two VMs eliminating a single point of failure.

> A disaster is a serious disruption involving widespread economic, environmental, or material loss that exceeds the ability of a cloud infrastructure to cope.

Disaster Recovery involves not only systems, but also a set of procedures, policies, tools, people, and partnerships to enable the recovery of critical applications following a disaster. A disaster is a serious disruption involving widespread economic, environmental, or material loss that exceeds the ability of a cloud infrastructure to cope. A prime example of a disaster is a fire in a data center compromising the physical servers and networking, but a more common example is ransomware. To ensure our systems can survive a disaster, we typically build a redundant system in a location far removed from the primary site so events such as weather, earthquakes, or meteors won't damage both systems. We also need to think in terms of risk distribution across technology or trust boundaries to ensure a resilient infrastructure.

Recovery Time Objective (RTO)/ Recovery Point Objective (RPO)

Before determining the appropriate DR strategy, you must first assess your business requirements for system availability. It's highly recommended that companies first perform a business impact analysis (BIA) to determine their recovery time objective (RTO) and recovery point objective (RPO). A BIA helps companies identify the operational and financial impacts that result from the disruption of business functions, systems, and processes.

Impacts that should be considered are:

- Contractual penalties
- Lost or delay of sales and revenue
- Regulatory fines
- Customer dissatisfaction
- Customer leaving for a competitor

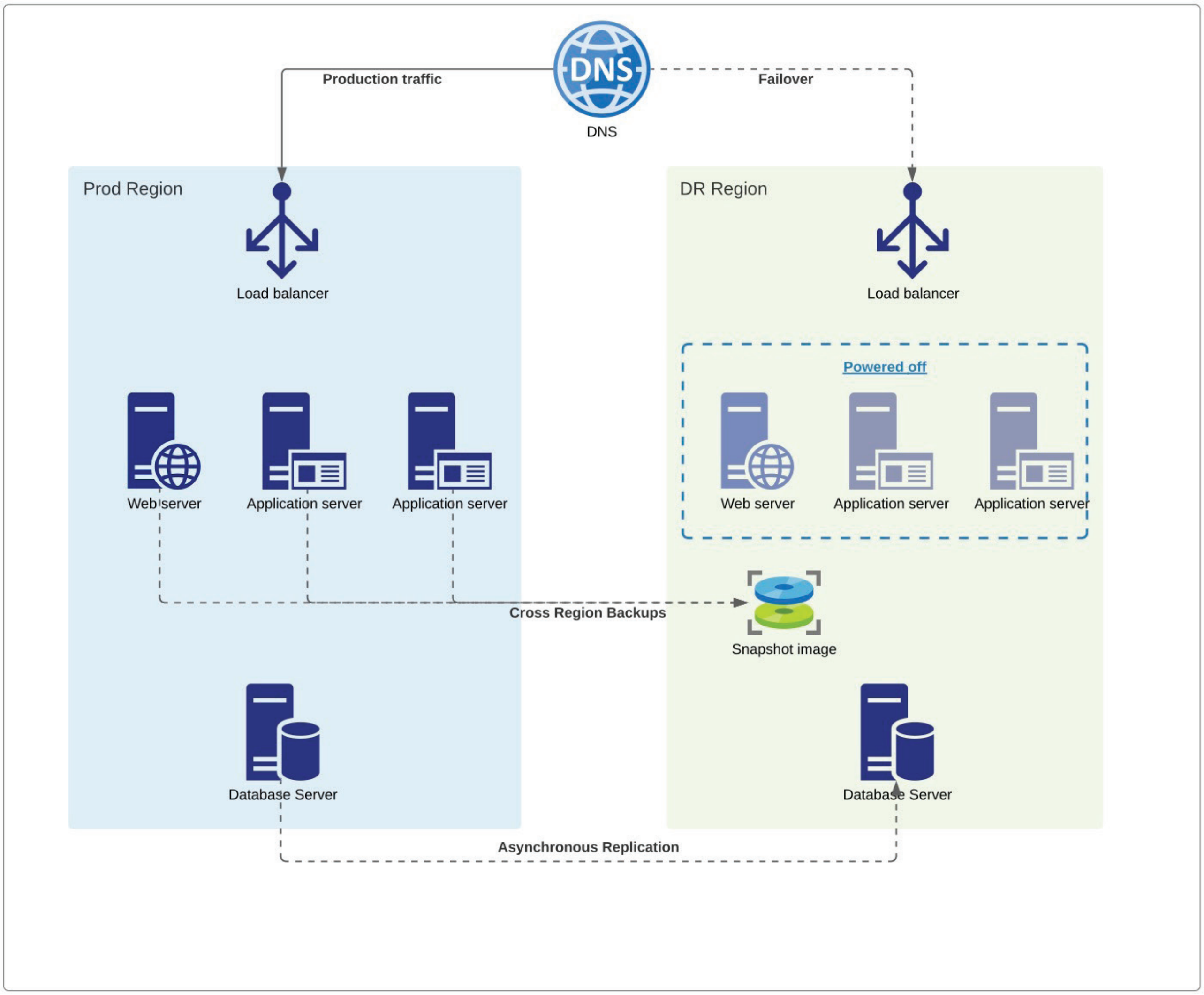
RTO refers to the amount of time it takes to return a system to an operational state after notification of a business disruption. For example, if an hour of downtime results in losing customers to competitors or paying significant fees due to breaching service level agreements, your business must be operationally ready before the end of the hour. In this case, the RTO requirement will be one hour.

RPO outlines how much data loss is acceptable in the event of a disaster. If losing an hour's worth of data will be detrimental to your company, backups should be taken every hour. Customers expect privacy, security, and durability of data shared with a company, and losing data is one of the quickest ways to lose customers to competitors.

Common DR Strategies

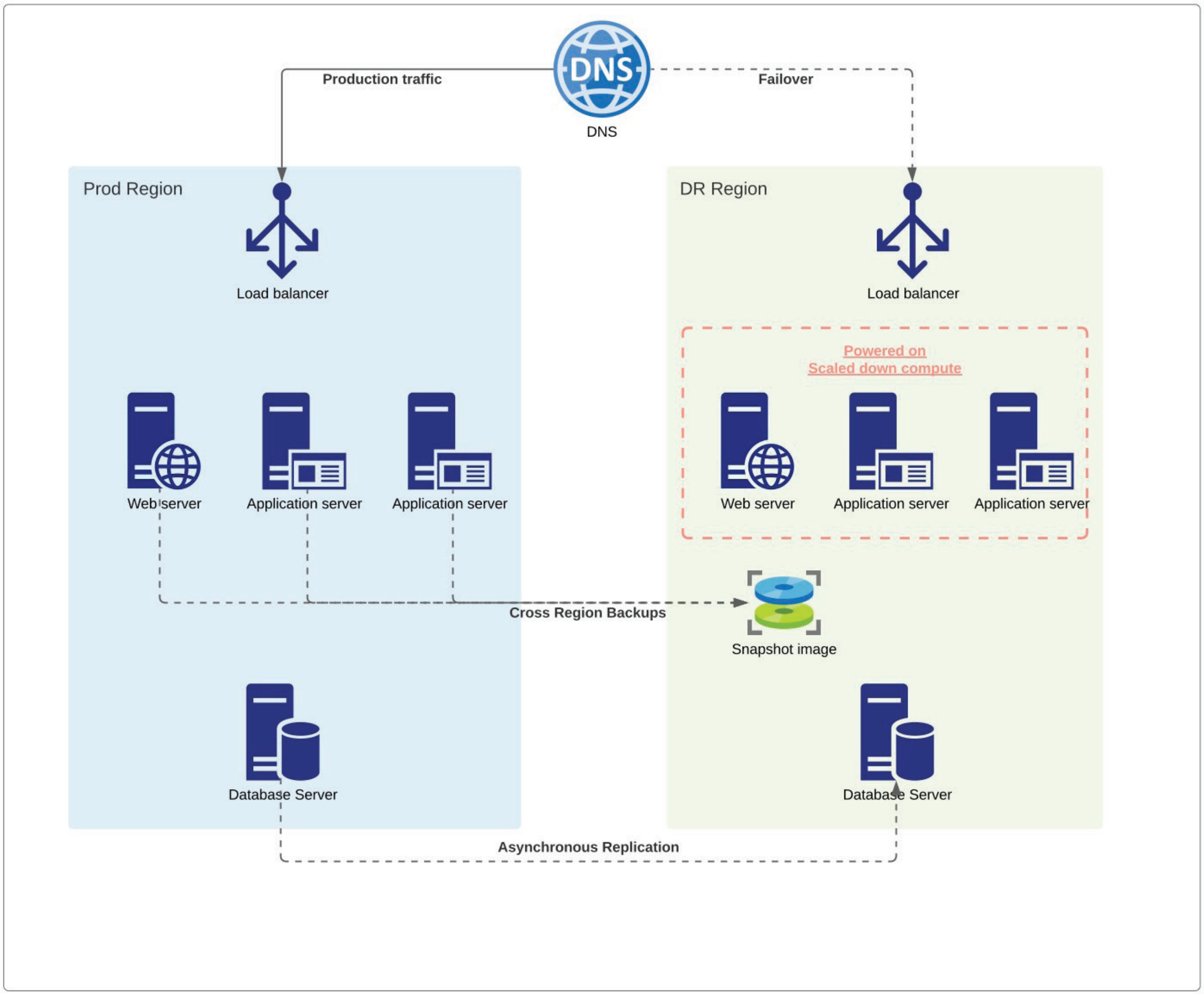
Pilot light

The term pilot light refers to a small flame that is always lit that enables a gas-powered appliance to start quickly. In the context of DR, it is used to describe a minimal scale remote site that contains the core system components with the latest configuration and critical data. Adopting this DR strategy reduces RTO and RPO over traditional backup and restore methods while being cost-efficient. We typically recommend customers start with this strategy.



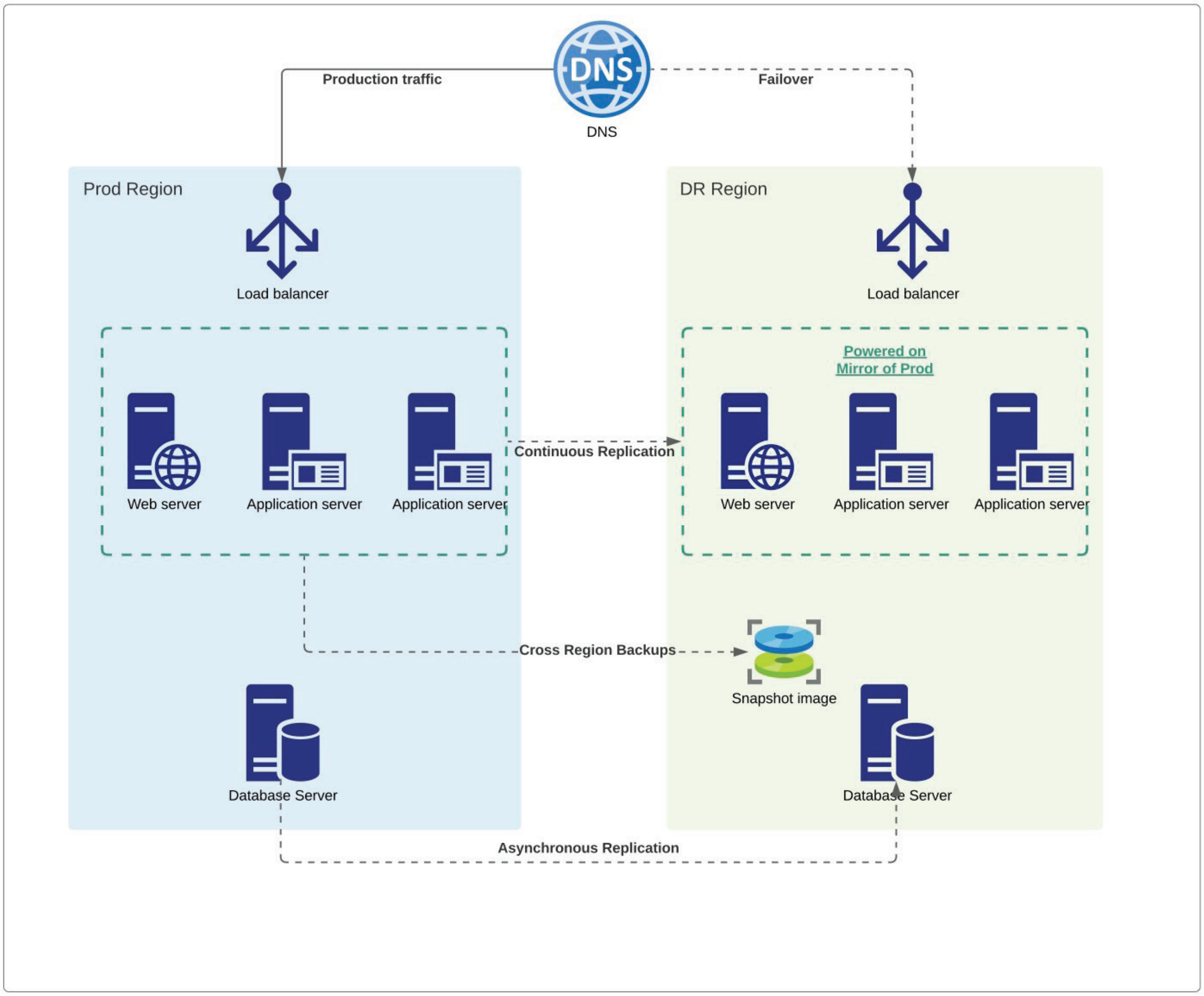
Warm standby

Warm standby expands on pilot light; it includes all components required for the production systems to successfully run on the DR site. The environment will be scaled down to save on cost but scaled-up in the event of a disaster to take over the load from the main site. Organizations can expect a lower RTO than a pilot light strategy and an increased cost of having a scaled-down, but production-ready system.



Hot Standby

A hot standby refers to a DR site that is a copy of the production environment and primed to take over on short notice. This is truly a fault-tolerant system with data continuously replicated from the primary site to the DR site. RTO is further reduced using this strategy to zero and with near-zero data loss. Hot standby allows companies to quickly failover but is the most expensive option.



Failback

An often-overlooked aspect in a Disaster Recovery strategy is failing back once the disaster has been resolved. Failback is the process of returning production systems to the original site and confirming they are in a ready state. For many organizations, defining, executing, and testing a failback strategy is not given the same level of effort as a DR failover. The best way to manage a failback is to build automation to handle the cutover and DNS configurations. Organizations who manually failback experience a 63% increase in their RTO as they start the transition back to the production site. There are cloud-native solutions; for example, CloudEndure for AWS, and Azure Site Recovery for Azure, that leverage automation wrapped in an easy-to-use GUI to simplify the process.

Test Your Plan

While having a DR plan is important, it only represents one step in the DR process. Proactively testing your plan allows you to train your engineers to quickly respond to a disaster, while reducing risk and increasing the effectiveness of data recovery. Organizations are often tempted to ignore this step due to the additional time, resources, cost, and potential disruption to production systems. However, in the event of a disaster, you will be thankful for having performed a DR test previously as it ensures a successful failover and failback. For government employees and contractors across Federal, State, and Local governments, the Cybersecurity and Infrastructure Security Agency offers an incident response training curriculum at no cost.

> Proactively testing your plan allows you to train your engineers to quickly respond to a disaster, while reducing risk and increasing the effectiveness of data recovery.

Summary

Whether you are a veteran of the cloud or just starting with a few running applications, having a robust Disaster Recovery strategy can allow your business to remain competitive and minimize revenue loss.

The insights gained after performing a BIA will help you determine the most suitable DR strategy to meet your business requirements. There are many DR solutions and strategies that fit the needs of any company. At the very least, if data and uptime are truly critical, implement a pilot light strategy. If you already have a DR plan, remember it is only as successful as your last DR test. Backup and test often, and in the event of a disaster, failover with confidence.

About Logicworks

Logicworks is a cloud consulting and managed services company that helps organizations plan, architect, and manage complex cloud environments. Our team of cloud experts have helped many organizations migrate to AWS and Microsoft Azure with our unique approach to cloud strategy and design.

As an AWS premier Consulting Partner and Azure Expert MSP with HIPAA, HITRUST, PCI, ISO 27001, SOC1, and SOC2 certifications, Logicworks specializes in complex workloads for companies with high security and compliance requirements.

If you're planning new cloud projects and want expert help in avoiding common migration stumbling blocks, visit www.logicworks.com or contact us at (212) 625-5300.

aws partner network

Premier
Consulting Partner

Security Competency
Migration Competency
Healthcare Competency
DevOps Competency
MSP Partner

HITRUST
CSF Certified

HIPAA COMPLIANCE

PCi

Gold
Microsoft Partner
Microsoft

Azure Expert MSP

ISO 27001

AICPA Service Organization Control Reports
AICPA SOC 1
Formerly SAS 70 Reports

AICPA Service Organization Control Reports
AICPA SOC 2
Formerly SAS 70 Reports