Protect Your Institution's Data From Operational Disruptions

Four Steps to Leveraging the AWS Cloud Adoption Framework for Security

With thousands of users entering sensitive data on thousands of disparate personal devices, schools and higher education institutions are among the most risk-sensitive organizations.

They face unique challenges to protect highly sensitive data and mission-critical applications. Those obstacles become even more acute in the event of natural disasters, technical failures, or security breaches. To minimize operational disruptions, reduce downtime from upgrades and updates, and more simply meet core security and compliance requirements, institutions are increasingly turning to the cloud.

Amazon Web Services (AWS) and our AWS Partner Network (APN) Education Competency partners offer hundreds of services and features specifically to help institutions meet their security objectives for visibility, auditability, control, and agility. Read below to walk through four steps for incorporating the AWS Cloud Adoption Framework (CAF) in order to protect your institution’s data from operational disruptions. You will see how to borrow from best practices we learned from our partners along the way.

1 Create Data Governance and Add Directive Controls

Governance is the unsung hero of cybersecurity and, with the recent surge in the number of institutions embracing digital learning, it's more important than ever. Data governance sets the foundation for understanding the needs of institutions, students, faculty, and staff, enabling them to adapt to changing conditions while still focused on their primary mission of providing education.

Many colleges and universities make the mistake of storing data without establishing clear data governance guidelines. But merely storing data is not enough. In many cases, institutions are not always aware of what data they have, where it is stored, or how sensitive or accurate it is. Without a governance program, the data is not useful or accessible and so-called data debt occurs. This means that organizations have to spend more time managing the increasing complexity of their environments instead of targeting resources.

Beyond the disorganization and lack of efficiency, there are also significant risks of having no data governance framework, including data breaches, misuse of data, and loss of corporate secrets and customer trust. As universities increasingly embrace integrating all of their data-direct sources, the subsequent increase in software as a service (SaaS) applications, Internet of Things (IoT), and artificial intelligence (AI) domains bring even more data requirements and complexity.

M&S Consulting, an APN Partner, sees the following common data challenges among higher education institutions:

» A growing amount of inconsistent business data that can be impossible to trust;

» Decreased organizational control, necessitating new data and analytics governance models that focus on trusting information as fit for purpose, rather than controlling the source information;

» Increasing demands on data integration, especially for critical needs such as master data management (MDM) and application data management (ADM).

> *"Data governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models. These describe who can take what actions with what information, and when, under what circumstances, using what methods."*

The Data Governance Institute

As a solution, M&S Consulting recommends that institutions create a foundational governance framework that includes consistent data definitions, data usage parameters, and security rules. Foundational governance frameworks ensure that plans are rooted in the participation of business, technology organizations, and executive support. When these processes are in place, universities can use the data collected and adjust their offerings quickly to adapt to changing environments.

A strong framework might contain the following elements:

» **Data classification.** This means identifying the types of data that are being processed and stored in an information system owned or operated by an organization.

» **Levels of sensitivity.** It also involves making a determination on the sensitivity of the data and the likely impact should the data be compromised, lost, or misused.

» **A single source of truth.** Establishing an agreed-upon source of truth minimizes duplication and excessive processing.

AWS provides several services and capabilities that institutions can use to implement, monitor, and enforce governance, including AWS Identity and Access Management (IAM), AWS Organizations, AWS Config, AWS Systems Manager, and AWS Service Catalog.

2 Implement Preventive Controls

When it comes to cloud infrastructure, the old maxim that "an ounce of prevention is worth a pound of cure" definitely rings true. That's why preventive controls are built into the AWS Cloud infrastructure, reducing the likelihood and impact of a threat or vulnerability. APN Partners provide extra protection by determining what changes your security architectures need and assisting with proper implementation. This enables your security teams to gain the confidence and capability needed to build necessary automation deployment skills. APN Partner Enquizit's Common App Refresh project offers an example of a reliable, secure system built using effective preventive controls.

The Common App Refresh

The Common App is a popular college admission application system that undergraduates use to apply to any of 900+ member colleges and universities across the globe. Common App knew that they needed to modernize their outdated, unnecessarily complex application system, so they tapped Enquizit's expertise for the project.

"The Common App Refresh was implemented as a cloud-native solution with no data center or non-cloud components," says TC Ratnapuri, chief executive officer, Enquizit. "And AWS was the most stable and mature choice available, offering enhanced out-of-the-box functionality and dynamic preventive controls."

With a focus on minimizing risks, Enquizit replaced the legacy system and delivered a new application with mission-critical performance at scale—along with elasticity, flexibility, security, and a lower total cost of ownership. A meta-directory in AWS serves as the app's foundation, with granular access managed through preventive controls such as policies, roles, and groups. End result? Common App now has the ability to control identity and access while also integrating with unique systems at hundreds of different universities.

> *"Preventive controls protect your workloads and mitigate threats and vulnerabilities."*

AWS Cloud Adoption Framework Security Perspective

3 Establish Guidance for Understanding Security and Compliance Postures

> *“While preventive controls play an important role in helping an organization become more resilient to attack, detection capabilities are critical for identifying ongoing attacks that may have evaded such preventive controls.”*
>
> Forrester Tech Tide Report, 2019

Now that you’ve put prevention measures in place, the next step is assuring you’re alerted in case the worst happens. With AWS, you can implement detection controls by processing logs, events, and monitoring in a way that allows for audits, automated analysis, and alarms. These controls are an essential part of the governance framework described in step one and can be used to support a quality process or compliance obligation, as well as for threat identification and response efforts.

Compliance is relevant for colleges and universities of all types and sizes. Although institutions have historically maintained one central IT department, specific organizations under a university’s umbrella face unique security and compliance needs. Research organizations are one example; those that work with federal agencies for research and execution of grants must meet specific National Institute of Standards and Technology (NIST) requirements. NIST 800-53 delineates security and privacy controls for federal information systems and organizations. When NIST introduces new versions, institutions are tasked with understanding how these changes impact their authority to operate (ATO). In practice, this means researchers at these universities must be able to prove that they have a NIST 800-53 compliant environment as part of the grant bidding and delivery process.

To help institutions reduce the time and cost of aligning with NIST requirements, APN Partner stackArmor developed the ThreatAlertTM Cloud Security System on AWS. ThreatAlert provides a comprehensive in-boundary solution that incorporates AWS best practices and services to secure data assets for compliance-focused organizations. It integrates and aggregates security and vulnerability data from various AWS services, such as AWS CloudTrail and Amazon GuardDuty, into a single dashboard. It also offers incident management and reporting services for customers to meet FedRAMP, FISMA, HIPAA, and PCI-DSS monitoring requirements.

4 Implement Responsive Controls to Reduce Harm and Restore Operations During and After a Security Incident

The last step in cloud security is making sure that your system gets back to normal after a harmful event and ensuring that the event will not repeat. To achieve this objective, responsive controls are needed to help reduce operational overhead and create repeatable, predictable approaches to monitoring and responding to events.

Here are some of the ways that AWS can help with disaster recovery (DR):

- By leveraging AWS Services, institutions might not need to purchase duplicate servers or maintain a duplicate data center.
- Automated machine conversion of source servers into AWS instances, and automated large-scale DR orchestration, mean that your recovery time happens in minutes or hours—launching all of your target machines in parallel on a mass scale.
- If your servers experience a virus, hacker, or ransomware attack that compromises your data, you can simply recover your data back to a specific point in time (i.e. point-in-time recovery).

Disaster Recovery as a Service (DRaaS)

With the increased worry of hackers and ransomware, many higher education institutions are choosing to outsource this burden. Through Disaster Recovery as a Service (DRaaS), APN Partner InterVision helps institutions mitigate the risk of ransomware by employing a recovery strategy that can bring your institution back online. InterVision's DRaaS services provides multiple recovery points to locate the most recent clean copy of data and a secondary recovery site to operate in. With this approach, systems can be restored outside of production to reduce the risk of forensic evidence loss or additional exposure.

Named a visionary in the 2019 Gartner Magic Quadrant for DRaaS, InterVision offers both assisted and fully managed DRaaS models which allow you to select the appropriate level of involvement for your institution's existing resources and objectives.

> *"Until recently, enterprise-grade disaster recovery had been prohibitively expensive for most organizations. Thanks to the rapid development of cloud infrastructure, organizations can now attain top-of-the-line disaster recovery capabilities into AWS at a fraction of the cost."*

AWS Disaster Recovery White Paper

Getting Help With AWS Cloud Security

Transitioning your college or university to the cloud is a monumental decision, and the security aspect is one of the biggest hurdles. But APN Partners offer hundreds of industry-leading security solutions that help institutions improve their security and compliance. Learn about products and solutions pre-qualified by the AWS Partner Competency Program to support you in multiple areas, which include infrastructure security, policy management, identity management, security monitoring, vulnerability management, data protection, and consulting services. With APN Partners, you can make sure you have a comprehensive security architecture in place so that your focus can remain on what you do best.