Athena Risk Assessment Report

Prepared by: Tiffany Christman

<u>Scenario</u>

Athena Learning Incorporated is an educational service provider. Athena has two major lines of business: course content creation and online learning services. Athena creates learning content and hosts learning content. Athena also provides internet sales services that enable its partners to charge their students to attend their courses.

Athena employs about 100 people in its headquarters office, and about 5 people each in its London and Singapore offices. Because it provides content and delivery services globally, Athena must comply with diverse privacy and security standards.

Athena serves as custodian for its own content and content that belongs to its partners. That content includes text, graphic, video, and interactive assets. This content is the essential intellectual property of the company. It also manages student account information including student registration, authentication, records, and payment information. Athena manages its own SQL databases, some of which are connected to web portals.

The Athena network consists of mostly MS Windows and Apple IOS clients with a mix of Microsoft and Linux servers to store business and employee records, learning content assets, and financial information, including customer data. The hosts include various PC brands and models of varying age. Different versions of operating systems are in use. Athena uses cloud services to deliver courses to the public, but must house assembled courses on the internal network for creation and editing. When the courses become available, they are mirrored to the cloud. Employees are permitted to use their personal phones and tablets for work. In addition, some employees work from home, but require full network access to do so. Athena also hosts its own DNS, email, and intranet services.

Athena employees use common office application software, custom applications, and tools that have been created internally.

Athena provides access to parts of its internal network to its partners through a secure web portal. Clients are able to preview their course content and deliver course assets to Athena for assembly in the Athena learning management system. Students interact with the cloud-managed learning platform through their web account logins.

Below is my assessment:

Information/Data Assets	Threats	Mitigation
Learning Content	Ransomware	EDR, isolate servers / backups
SQL databases	SQL injection	Input validation and Output encoding
Employee Records	Credential Theft	MFA
Payment Information	Keylogger	Allowlisting

Software Assets	Threats	Mitigation
Windows and Mac IOS	Virus	EDR
Cloud Services	IAM credentials allowing too much access	Least Privilege IAM
Courses	Trojan	User / Admin Separation

Physical Assets	Threats	Mitigation
Microsoft / Linux Servers	DoS / DDoS	Rate limiting
Various PC Models	Device Theft	Cameras / Visitor logs
Headquarters	Unauthorized access	Mantraps

Network Assets	Threats	Mitigation
DNS	DNS spoofing	Use trusted recursive resolvers
VLAN	ARP spoofing	Dynamic ARP Inspection
Firewalls	No inbound rules, "Allow any"	Use SSH / HTTPS

Aligned with NIST Cybersecurity Framework & CIS Controls