

7/27/2024

Cloud Computing Assignment

Report on a Proposed AWS Cloud Computing IT System for a School with Outdated IT Infrastructure.

Author: S275931
UNIVERSITY OF SUFFOLK

Cloud Computing Assignment

Table of Contents

Executive Summary	2
Introduction	2
Literature Review.....	3
Background	3
Benefits of using Cloud Based Technologies for School IT Systems.....	3
Considerations for using Cloud Based Technologies for School IT Systems	4
Comparing Amazon Web Services with Other Cloud Computing Platforms.....	5
AWS Educational Products.....	11
Case Study	12
Cloud Readiness Assessment.....	12
Business.....	12
People	13
Governance	13
Platform	13
Security	13
Operations.....	14
AWS Cloud Solution	14
Findings and Recommendations	25
Findings	25
Recommendations.....	28
Road plan for Implementation.....	31
Conclusion.....	33
References.....	34
Appendix	37
Appendix A: Benefits of using Cloud Based Technologies for School IT Systems.....	37
Appendix B: Considerations, Drawbacks and Using AWS for School Cloud Computing Platforms.....	40
Considerations for using Cloud Based Technologies for School IT Systems	40
Disadvantages of using Cloud Based Technologies for School IT Systems	40
Using Amazon Web Services for School IT Systems	42
Appendix C: AWS Educational Products.....	43

Appendix D: Cloud Readiness Assessment.....	45
Business	46
People.....	47
Governance.....	48
Platform.....	48
Security.....	49
Operations	51
Appendix E: Cloud Recommendations.....	52
Appendix F: Full Cloud Readiness Assessment Report	55

Executive Summary

This report is about the implementation of a cloud-based IT system and infrastructure in a secondary school and sixth-form college in the UK that is facing several problems because of its current outdated IT system. The school's current IT system is outdated and uses obsolete hardware and software and faces quality-of-service issues, no disaster proofing with no data backups, outdated cybersecurity software, performance issues and is slow resulting in inefficient teaching, learning and school administration and management. Due to the limitations of the school's budget and insufficient government funding, the school is having financial difficulties trying to upgrade its on-site IT infrastructure the traditional way therefore the cloud-based IT infrastructure proposal will save the school time and money while providing the school with the latest IT technologies and upgrading the IT systems. It is recommended that the school adopts a cloud-based IT infrastructure system using Amazon Web Services (AWS) to reduce upgrade costs, improve efficiency of teaching, learning and administration, improve security and reliability of the IT system, provide assistive technologies for students with special needs and for digital preservation of schoolbooks.

Introduction

This report is a case study for a secondary school with a sixth form college in the UK that has an outdated IT system and infrastructure and proposing a cloud-based solution to resolve these problems that includes the AWS architecture diagram of the proposed system. The current IT system is facing several problems including old and slow servers and computers, outdated hardware and software, no disaster proofing or backups, outdated cybersecurity measures, no remote access, no video conferencing or collaboration tools, grades, student records and paperwork being processed in local spreadsheets or documents and an outdated and user-hostile website. The proposed solution is to develop a cloud-based school IT system using Amazon Web Services

(AWS) to provide the school with a new IT system that is faster, up to date software, more reliable, automated, more efficient, more secure and with more useful features than the current system.

Literature Review

Background

The school is currently facing problems with its current outdated IT system that is slow, unreliable, uses obsolete technology, has quality of service and compliance issues, no disaster proofing, outdated cybersecurity, no efficient school administration tools and provides no innovative learning environments. Research into a cloud-based IT system for the school has resulted in the recommendation for a cloud-based solution for this school using Amazon Web Services (AWS) as other schools are using cloud technologies for their IT systems with successful results.

Benefits of using Cloud Based Technologies for School IT Systems

For full details see [Appendix A: Benefits of using Cloud Based Technologies for School IT Systems](#)

There are several benefits of using Cloud Based Technologies for a school IT system that include:

- Economic benefits – schools can utilise cloud-based IT systems to save money by using free cloud-based software instead of expensive traditional proprietary software, lower school electricity bills by not needing to power on-site server equipment and more powerful and power-hungry computers, not needing to purchase expensive on-site server hardware and software, utilising cheaper cloud-only devices, using pay-as-you-go and monthly subscriptions for SaaS, PaaS and IaaS. Lifespan of existing IT infrastructure is extended using cloud-based technologies (Department for Education, 2019). Data storage costs are also reduced (HubVela, 2023).
- Efficiency benefits – saves teachers', students' and staff time by using school software from any device at any time and place, improving collaboration between staff and students using collaborative software and sharing resources and easier access to curriculum resources (Department for Education, 2019). Cloud computing also improves efficiency by automating tedious school and IT administration and management tasks, constant access to learning and teaching materials for teachers and students and administration tools for staff, replacing textbooks and library books with e-books to reduce the risk of loss and damage, and allows teachers to host online classes (HubVela, 2023).

- Cloud computing improves the effectiveness of school IT systems by using automation to reduce workload on school IT administrators and technicians, provides backup and disaster recovery options (Department for Education, 2019) and enhanced data storage and management to help prevent data loss (HubVela, 2023). Cloud computing provides enhanced cybersecurity for school IT systems by utilising firewalls, IAM roles, security groups and hardened containers and operating systems (Morris, 2023).
- Learning and Teaching – Cloud computing is beneficial to learning and teaching in several ways including tailoring learning experiences and environments to meet individual student's needs, using artificial intelligence and machine learning to analyse student data, classwork, assignments, homework and grades to provide teaching and other recommendations to school staff, allow feedback to students by teachers and access to a wider range of learning materials (HubVela, 2023).
- Special Needs Assistance – Cloud computing provides assistive technology for students with special needs and disabilities as well as those without disabilities. Cloud computing allows assistive software to be deployed rapidly and is accessible to all students resulting in disabled students having greater independence, opportunities and mobility (HubVela, 2023).

Considerations for using Cloud Based Technologies for School IT Systems

For full details see [Appendix B Considerations, Drawbacks and Using AWS for School Cloud Computing Platforms](#).

There are considerations that the school needs to consider when leveraging a cloud-based IT system. These include the school's internet connection (a reliable hyper fast full-fibre dedicated leased line is required) to connect to cloud services, the speed of the school's on-site networking equipment, acceptance of the cloud-based IT systems by members of staff and students, compatibility with on-site IT infrastructure and the financial feasibility of upgrading to a cloud-based system. Data protection, cybersecurity, privacy and online safety must be considered due to the sensitive data and child-generated content stored on the school IT systems and therefore must comply with the Data Protection Act 2019, Computer Misuse Act 1990 and Online Safety Act 2023 (Department for Education, 2019).

There are reasons to use Amazon Web Services (AWS) for a cloud-based for a school IT system that include elasticity and scalability to dynamically adjust computing resources depending on demand as well as providing data protection, privacy and cybersecurity tools including Identity Access Management (IAM), firewalls, encryption, security groups, backup and recovery services. Pay-as-you-go and subscription

services eliminates needing expensive software licenses, on-site hardware upgrades and requires fewer IT staff (Roman Ceresnak, 2024). AWS Academy and AWS Educate provide cloud computing training providing students with qualifications and career opportunities. AWS can host educational, teaching, learning and online class applications. Schools can build custom IT infrastructure on AWS to meet the school's needs and be managed by a services provider (Jones, 2022).

There are disadvantages of a cloud-based school IT system/infrastructure that include reliability and downtime concerns – if there is server downtime or no internet connection then the school IT infrastructure and systems are unavailable. Another concern is privacy and cybersecurity as sensitive school data will be hosted on external cloud servers instead of locally, increasing the risk of data breaches and cyberattacks as data centres are more likely to attacked than local school servers. Vendor lock-in makes it difficult to change cloud provider. Managing multiple cloud platforms for different IT systems is complex and cloud-based school technologies more computer literate users. Furthermore, the school has little control over its data once its uploaded to cloud servers compared to local school servers because cloud servers are owned, managed and monitored by the cloud computing provider. Finally, there is a learning curve with cloud computing technologies that requires administrator and user training for the cloud-based IT systems and will be difficult for computer illiterate people and those without access to technology (HubVela, 2023).

Comparing Amazon Web Services with Other Cloud Computing Platforms

Table to compare Amazon Web Services with other cloud computing platforms including Microsoft Azure and Google Cloud Platform.

Feature	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Summary	Leader in Cloud Computing – Massive range of tools from computation to data storage (Dhaduk, 2022).	Easy to integrate with the Microsoft ecosystem – Hybrid cloud solutions, Azure virtual machines, Blob storage (Dhaduk, 2022).	Focus on data analytics and innovation – GCP Big Query and TensorFlow are leading data science, Machine Learning and AI technologies (Dhaduk, 2022).
Advantages	<ul style="list-style-type: none"> • More tools and services than competitors. • Most established 	<ul style="list-style-type: none"> • Supports hybrid cloud systems. • Good integration with other 	<ul style="list-style-type: none"> • Simple pricing and low-cost. • Leading artificial intelligence, machine

	<p>cloud computing platform.</p> <ul style="list-style-type: none"> • Reliable data transfer. • More experts than competitors. • More computational resources than competitors • Good documentation (Dhaduk, 2022). • Best for reliability and security (Coursera, 2024) 	<p>Microsoft products.</p> <ul style="list-style-type: none"> • Available in many countries and regions. • Comprehensive range of developer tools (Dhaduk, 2022). • Good artificial intelligence, machine learning and analytics services. • Cheaper than AWS and GCP • Good support for hybrid technologies (Coursera, 2024). 	<p>learning and data science.</p> <ul style="list-style-type: none"> • Compatible with Google APIs and Kubernetes. • Migrate live virtual machines (Dhaduk, 2022). • Good support for containerisation (Coursera, 2024).
Disadvantages	<ul style="list-style-type: none"> • Complicated pricing structure. • Inferior hybrid cloud strategies (Dhaduk, 2022). 	<ul style="list-style-type: none"> • Compatibility issues when integrating with non-Microsoft products. • User-Hostile user interface (Dhaduk, 2022). 	<ul style="list-style-type: none"> • Narrow range of products. • Available in fewer countries and regions. • Support for enterprises is limited (Dhaduk, 2022).
Computing	<ul style="list-style-type: none"> • Elastic Cloud Compute (EC2) • Auto Scaling • Hardware accelerated computing using 	<ul style="list-style-type: none"> • Azure Cloud Computing Service • Large network of virtual machines based on open-source 	<ul style="list-style-type: none"> • Google Compute Engine • Google Kubernetes Engine • Google Cloud Functions

	<p>Graphics Processing Units (GPUs)</p> <ul style="list-style-type: none"> • Burstable performance instances. • Compute optimised virtual machines • Elastic Container Service (ECS) with Docker. • AWS Batch • AWS LightSail • AWS Elastic Beanstalk • AWS Lambda • Elastic Load Balancing • AWS Serverless Application Repository (Dhaduk, 2022). 	<p>cloud platforms</p> <ul style="list-style-type: none"> • Compatible with Windows and Linux servers. • Compatible with third party platforms including Oracle and SAP. • Good for hybrid clouds. • Azure Batch • Azure Infrastructure-as-a-Service (IaaS) • Service Fabric • Azure Platform-as-a-Service (PaaS) • Azure Spring Cloud • Azure Functions • Azure Kubernetes Service (AKS) (Dhaduk, 2022). 	<ul style="list-style-type: none"> • Google App Engine (Dhaduk, 2022).
Region Availability	<ul style="list-style-type: none"> • 22 geographic locations and 14 data centres, 114 edge locations, 12 regional edge caches 	<ul style="list-style-type: none"> • 54 regions with 3 availability zones each, 116 edge locations (Coursera, 2024) 	<ul style="list-style-type: none"> • 34 cloud regions, 103 zones, 200+ edge locations (Coursera, 2024).

	(Coursera, 2024)		
Machine Learning and Artificial Intelligence	<ul style="list-style-type: none"> • Amazon Transcribe • Amazon Polly • Amazon Lex • Amazon Translate • Amazon Comprehend • Amazon Rekognition • Amazon Lookout Family Fraud Detector • Amazon Personalize • SageMaker Autopilot • SageMaker Studio • SageMaker MLOps (Dhaduk, 2022). • Gluon (Coursera, 2024) 	<ul style="list-style-type: none"> • Speech to Text • Test to Speech • Language Understanding • Translator • Text Analytics • Computer Vision Face Indexer • Metrics Advisor • Personalizer • Automated ML • Machine Learning Notebooks • MLOps (Dhaduk, 2022). • Bing web search API (Coursera, 2024) • Face API • Custom Vision Service (Coursera, 2024) 	<ul style="list-style-type: none"> • Speech to Text • Text to Speech • Dialogflow • Translation • Natural Language • Vision, Video • Cloud Interface • Recommendations AI • AutoML • AI Platforms • Pipelines (Dhaduk, 2022). • TensorFlow (Coursera, 2024)
Storage	<ul style="list-style-type: none"> • Amazon Simple Storage Service (S3) Buckets • Amazon Elastic Block Store (EBS) • Amazon S3 Glacier 	<ul style="list-style-type: none"> • Blob Storage • Managed Disks • Azure Archive Blob Storage • Azure File Storage (Dhaduk, 2022). 	<ul style="list-style-type: none"> • Google Cloud Storage • Google Compute Engine Persistent Disks • Google Cloud Storage Nearline • ZFS/Avere (Dhaduk, 2022).

	<ul style="list-style-type: none"> Amazon Elastic File System (Dhaduk, 2022). 		
Security	<ul style="list-style-type: none"> Granular Identity Access Management (IAM) and Firewalls isolate data. Assess vulnerabilities using AWS inspector API Activity Monitoring Guard Duty for threat intelligence (Dhaduk, 2022). 	<ul style="list-style-type: none"> Central Security System. Anti-malware protection for malware protection. 256-bit AES encryption for Azure Keys Penetration tests to test security measures (Dhaduk, 2022). 	<ul style="list-style-type: none"> Security from privileged access attacks. Google KMS to manage cryptographic keys Google Identity Access Management (IAM) for granular access control. Google Cloud Security Scanner to detect potential threats (Dhaduk, 2022).
Pricing	<ul style="list-style-type: none"> 12 months free: AWS EC2, AWS S3, AWS Relational Database Service (RDS) (SQL) Trials: Amazon SageMaker, Amazon Redshift, Amazon App Stream 2.0 Always Free: AWS DynamoDB, AWS Lambda, Amazon Simple Notification 	<ul style="list-style-type: none"> 12 months free: Azure Virtual Machines – Windows/Linux, Azure Blob Storage, Azure SQL Database Trials: N/A Always Free: Azure Cosmos DB, Azure Functions, Azure Event Grid Minimum Instance: 2 vCPUs, 8GB RAM, \$70 per month. 	<ul style="list-style-type: none"> 12 months free: N/A Trials: Google Kubernetes Engine, Compute Engine, Firestore, Cloud Functions Always Free: N/A Minimum Instance: 2 vCPUs, 8GB RAM, \$52 per month. Maximum Instance: 160 vCPUs, 3.75 TB RAM, \$5.32 per hour (HubVela, 2023).

	<ul style="list-style-type: none"> Service (SNS) • Minimum Instance: 2 vCPUs, 8GB RAM \$69 per month • Maximum Instance: 128 vCPUs, 3.84 TB RAM, \$3.97 per hour (Dhaduk, 2022). • Price per second basis with minimum of 1 minute. 	<ul style="list-style-type: none"> • Maximum Instance: 128 vCPUs, 3.89 TB RAM, \$6.97 per hour (Dhaduk, 2022). • Per minute basis 	<ul style="list-style-type: none"> • Per minute basis
Notable Users	<ul style="list-style-type: none"> • Coursera • Netflix • Coca Cola • Coinbase • Expedia • Intuit • Airbnb • Lyft • US Food and Drug Administration (FDA) (Coursera, 2024) 	<ul style="list-style-type: none"> • Bosch • Audi • Hewlett Packard (HP) • HSBC • 3M • FedEx • Mitsubishi • Renault • Starbucks • ASOS (Coursera, 2024) 	<ul style="list-style-type: none"> • Spotify • Nintendo • X/Twitter • PayPal • UPS • Toyota • Equifax (Coursera, 2024)
Hybrid and Multi Cloud	<ul style="list-style-type: none"> • Amazon ECS Anywhere • AWS Snowcone • AWS Snowball • AWS Snow Mobile • AWS Outposts 	<ul style="list-style-type: none"> • Azure Arc • Azure Backup • Azure Active Directory • Azure Security Centre • Azure Blob Storage • Azure Stack • Azure Sentinel 	<ul style="list-style-type: none"> • Anthos • Traffic Director • Looker • Cloud Build • Operations • Cloud Run for Anthos (Coursera, 2024)

	<ul style="list-style-type: none"> • VMware Cloud on AWS • AWS Wavelength • AWS EKS Anywhere (Coursera, 2024) 	<ul style="list-style-type: none"> (Coursera, 2024) • Windows Server Backup • Visual Studio integration (Coursera, 2024) 	
--	--	---	--

AWS Educational Products

For full details see [Appendix C: AWS Educational Products](#).

Amazon Web Services (AWS) provides a comprehensive range of educational, administration and management tools for schools and educational institutions that are reliable, scalable, secure, innovative and provide remote learning opportunities. These products include (Amazon Web Services, 2024):

- Remote and Virtual Learning software (Amazon Web Services, 2024).
- Data Modernisation and Backup Tools (Amazon Web Services, 2024).
- Artificial Intelligence (AI), Machine Learning (ML), Business Intelligence, Data Science and Natural Language Queries to find required data more quickly for school management, planning and performance metrics (Amazon Web Services, 2024).
- Scalable and secure Student Management Solutions (Amazon Web Services, 2024).
- AWS Ransomware Mitigation and Disaster Recovery Tools (Amazon Web Services, 2024).
- Data Analytics Tools (Amazon Web Services, 2024).
- Contact Centre (Amazon Web Services, 2024).
- Learning Management System (Amazon Web Services, 2024).
- Core Administrative Systems (Amazon Web Services, 2024).
- Data Management Solutions (Amazon Web Services, 2024).
- Identity Access Management (IAM) for security (Amazon Web Services, 2024).
- Infrastructure Modernisation Solutions (Amazon Web Services, 2024).
- Security, Risk and Compliance solutions (Amazon Web Services, 2024).
- Admissions and Financial Aid Processing solutions (Amazon Web Services, 2024).
- Student Communication Tools (Amazon Web Services, 2024).
- Library Catalogue Management Solutions (Amazon Web Services, 2024).
- Digital Preservation Solutions for books (Amazon Web Services, 2024).

- Virtual Proctoring Solutions for exams (Amazon Web Services, 2024).

Case Study

A U.S. K-12 school district leveraged Amazon Web Services (AWS) to provide a robust virtual learning and classroom environment where students and teachers can seamlessly interact.

Students were able to use any internet connected device to access their educational resources, coursework, homework, and classwork. The students were able to learn at their own pace due to the flexibility of the AWS system and ended the need to use physical textbooks and materials. The collaboration tools on AWS allowed the students to work together on classwork and group projects and improved communication and teamwork skills.

AWS in the school district simplified administrative tasks including attendance monitoring and assignment grading. Teachers are more able to focus on quality teaching and personalised learning experiences due to automated administrative processes and centralised data storage (Roman Ceresnak, 2024).

Cloud Readiness Assessment

The AWS cloud readiness assessment (CRA) conducted for the school regarding its outdated IT systems/infrastructure has shown that the school would benefit from a cloud-based IT system and infrastructure due to the low CRA score because of using substandard IT infrastructure. The CRA is split into six sections – Business, People, Governance, Platform, Security and Operations (Amazon Web Services, 2024).

Full Cloud Readiness Assessment available here: <https://cloud-computing-diagrams.onrender.com/static/CRA-Report.pdf>

For full details see [Appendix D: Cloud Readiness Assessment](#).

Business

Business includes the school exploring new cloud-based technologies to overcome technical debt caused by their outdated and substandard IT systems and infrastructure. Consider financial and non-financial benefits of implementing a cloud-based IT system and prioritise strategic objectives over time to embrace technology advancements and use automated discovery tools to migrate applications to the cloud. Agile methodologies and CI/CD pipelines will streamline application and IT system development and adapts quickly to changes. Use data analytics, artificial intelligence and machine learning to obtain data for diagnostics and troubleshooting and non-technical data for tracking student, teacher and school performance - must comply with the Data Protection Act 2018 due to the confidential data in schools.

People

People includes incorporating new behaviours and mindsets to attract, retain and empower staff to use agile methodologies, reducing bureaucracy and enabling innovation and rapid decision making. School IT administrators need training in cloud fluency so they can develop, orchestrate, maintain and manage the AWS cloud-based school IT system. Modernise school leadership into a transformational and cross-functional cloud leadership to increase acceptance of new ways of working to accelerate cloud adoption. Identify key stakeholders, risks, cross-organisational dependencies and barriers and create change and risk management plans. Develop a centralised evolving team with a top-down approach to drive desired outcomes and stop functional silos.

Governance

Governance includes frequently validating the roadmap with the project sponsors of the school cloud-based IT system and escalate issues to the steering committee. Assess and identify risks and create a risk management plan that uses cloud-based services to manage and respond to risks. Clarify roles and responsibilities on the school cloud IT systems and make sure the steering committee and project sponsor have understood the costs. Cloud services save the school money by using dynamic forecasting budgeting, financial anomaly detection, consolidated and simplified cloud billing and centralised cloud software and license management. An accurate and complete application inventory minimises inventory sprawl and assists with cloud transformation. Ensure that the cloud-based IT system complies with legislation that applies to schools.

Platform

Platform includes developing a well architected cloud environment for the school IT systems and infrastructure to accelerate implementation, reduce risks, costs, complexity and technical debt, then develop and deploy blueprints and guardrails for authentication, networking, security, centralised logging and monitoring. Use a hybrid cloud to integrate on-site infrastructure with cloud infrastructure, for backups and disaster recovery, cloud bursting, edge computing and distributed data processing. Decide which workloads to migrate to the cloud. Automate IT workflows, use microservices, containers and serverless technologies to optimise resource allocation, automated scalability and simplification. Use DevOps and CI/CD pipelines with staging and production steps and testing to streamline development.

Security

Security includes identifying relevant laws for data protection, cybersecurity and online safety for schools and giving staff training for cybersecurity and awareness of their roles and responsibilities. Use Identity and Access Management (IAM) to define user roles to

prevent unauthorized access to restricted resources. Use firewalls to block harmful and illegal online content. Use virtual private clouds and private subnets to host private cloud components and use security groups. Regularly use cybersecurity software, automation and ML to scan for vulnerabilities, exploits and new threats, then automatically patch software. Improve application security by finding and fixing vulnerabilities during the coding phase. Encrypt files and data, use principle of least privilege and zero trust for data protection.

Operations

Operations include developing a dashboard that gives a unified view of the school's IT system's performance by using telemetry and canaries (scheduled scripts) to monitor the internal state of the school's cloud IT systems for diagnostics and troubleshooting. Use cloud-based automation, AI and ML to detect, manage and respond to threats, anomalies and incidents. Use deployment management systems to track, test and implement changes then analyse results to reduce deployment failures and automate rollbacks. Develop a disaster recovery plan that includes scheduled data backups and assess risks and severity of different disaster scenarios. Consolidate operation and management systems onto a single IT systems management console that including applying scheduled software patches.

AWS Cloud Solution

An AWS architectural diagram has been created featuring the components of the proposed cloud-based school IT system. The list of features are in the list below the AWS architectural diagram.

AWS Diagram available here: <https://cloud-computing-diagrams.onrender.com/>

AWS Diagram also available here: <https://cloud-computing-diagrams.onrender.com/awsarchitecturediagramhtml>

Amazon Web Services (AWS) Architecture Diagram for School I.T. System. Authour: S275931

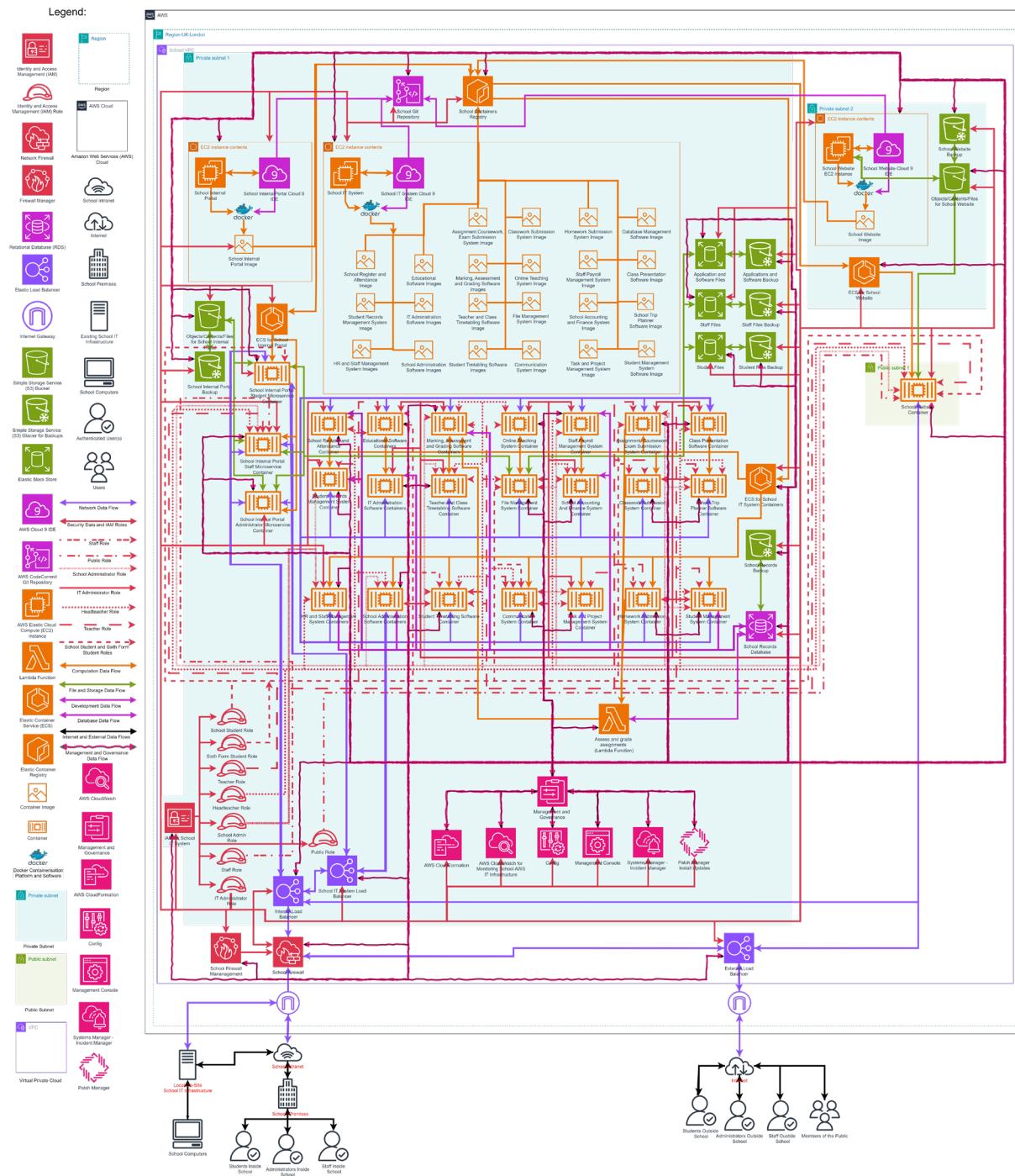


Figure 1 - Amazon Web Services architecture diagram for the school IT system. Zoom in to view content.

The table lists the components used in the AWS cloud-based school IT system and infrastructure.

Component	Description				
Amazon Web Services	Computing platform to host IT system and its infrastructure and applications				
Region	Amazon Web Services computing platform to host IT system and its infrastructure and applications.				
School VPC	Virtual Private Cloud that provides the virtual network for the school IT systems on AWS				
Private Subnet 1	Hosts the school's IT system, internal website and portal, and the different school IT applications as containers and lambda functions. This also includes the EC2 platform to develop the applications, the CodeCommit Git repository, the Elastic Container Registry, the Elastic Container Services, Simple Storage Service (S3) buckets, Elastic Block Storage (EBS), S3 Glacier backups, School database, the firewall, Identity and Access Management and AWS Management and Governance features. Portal is accessible inside the school premises intranet through authentication. The school portal is accessible outside the school premises through user authentication.				
Private Subnet 2	Hosts the school the EC2 instance for the school's website development and its S3 Buckets and Glacier backups.				
Public Subnet 1	Public subnet for the container hosting the school's external website that is accessible to the public outside of the school premises.				
Firewall	Prevent unauthorised malicious access to the School's AWS IT systems, blocks cyberattacks and hackers, blocks inappropriate websites, social media, age restricted, offensive, and harmful content being accessed in the school, blocks students from accessing distracting content such as social media, unauthorised communications, game websites, TV, video and movie streaming websites especially during class, blocks access to malware websites and malicious downloads.				
Firewall Management	Firewall Management – Manage firewall settings such as what content to block, restrict and unblock.				
Identity and Access Management (IAM)	Provide security by restricting access to components of the AWS school IT system and applications based on user roles <table border="1"> <thead> <tr> <th>IAM Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>IT Administrator Role</td><td>Full access to all components and applications of the AWS school IT system and AWS cloud management including: <ul style="list-style-type: none"> • EC2 instances for developing school IT system • CodeCommit repository • ECR container registries • Cloud Governance and Management tools • S3 Buckets </td></tr> </tbody> </table>	IAM Role	Description	IT Administrator Role	Full access to all components and applications of the AWS school IT system and AWS cloud management including: <ul style="list-style-type: none"> • EC2 instances for developing school IT system • CodeCommit repository • ECR container registries • Cloud Governance and Management tools • S3 Buckets
IAM Role	Description				
IT Administrator Role	Full access to all components and applications of the AWS school IT system and AWS cloud management including: <ul style="list-style-type: none"> • EC2 instances for developing school IT system • CodeCommit repository • ECR container registries • Cloud Governance and Management tools • S3 Buckets 				

		<ul style="list-style-type: none"> • S3 Glaciers • Elastic Block Stores • School Database • Load Balancers • Elastic Container Service • Docker • Cloud9 • All containers and images • Firewall settings • Internet Gateways • Private and Public Subnets • Region • Identity and Access Management • Make changes to and modify the AWS school IT systems. • Add and remove applications from school IT systems.
	Public Role	The most restricted user role that for unauthenticated members of the public looking at the school's website. This IAM role only allows members of the public to access the school's website and nothing else. The public cannot access the school portal, containers, AWS management or any files.
	Student Role	<p>The second most restricted user role used by the secondary school students. They can only use the AWS container applications relevant to their schoolwork including:</p> <ul style="list-style-type: none"> • School Student Portal • Educational software containers to complete classwork and homework for lessons. • Student timetable container to view their timetables • File management container – access to files available to students only. • Communications Container – Communication between students and teachers. Monitored to prevent abuse. Filters used to report and prevent profanity and abusive language, images and videos being sent. • Assignment, classwork and homework submission containers – submit assignments, classwork and homework only.

		<ul style="list-style-type: none"> • Access to external school website. • Restricted internet access to prevent access to malicious, inappropriate, offensive or harmful content. • Not allowed to change settings on AWS or perform administrative tasks. • Not allowed to access containers, applications, database or files that are for staff only.
	Sixth Form Role	Similar to Student Role but with slightly fewer restrictions.
	Teacher Role	<p>Teachers have access to the following:</p> <ul style="list-style-type: none"> • All the containers students have access to however with more functionality such as viewing all students' assignments, classwork, homework and timetables. • File Management Container – Teachers have access to staff and student files. • School Register and Attendance container • Student Records Management Container • Staff Internal Portal Management Container • Communication system container with fewer restrictions and more features. • Teacher and Class Timetabling Software Container • Educational software Container (access to more apps than students with fewer restrictions) • Marking, Assessment and Grading Software Containers • Online Teaching System container to orchestrate online classes • Student Management System Container • School Trip Planner Container • Class Presentation Software Container • Less restricted internet access however seriously harmful and illegal content will still be blocked. Hacking and malware websites will still be blocked. • Make some changes to some containers to suit classes and assignments.
	Headteacher Role	<p>Headteacher has access to the following:</p> <ul style="list-style-type: none"> • All containers, features, components and applications students and teachers have access to.

		<ul style="list-style-type: none"> • Internal portal staff microservice • School Administration Software containers • Access to student and staff files • Task and Project Management System Container • School Accounting and Finance Container • Staff Payroll Management System Container • Student and Staff Files • Less restricted internet access than students however illegal, seriously harmful content and malware are still blocked. • Can make more changes than students, teachers, school administrators and other staff to the school management and IT systems however technical changes and changes directly affecting the operation of the AWS cloud system will still need to be done by the IT administrators.
	School Admin Role	<p>School administrator staff have access to:</p> <ul style="list-style-type: none"> • Student Records Management System Container • School Administration Software Containers • Marking, Assessment and Grading Software Containers • Teacher and Class Timetabling Software Containers • Communication System Container • File Management System Container – Student and Staff Files • Staff Payroll Management System Container • School Accounting and Finance System Container • Task and Project Management System Container • School Trip Planner Software Container • Student Management System Container • Less restricted internet access than students, however illegal, seriously harmful, malicious content and malware is still blocked. • Can make more changes and use more features than students but cannot make as

		many changes as the IT administrators or headteacher.
	Staff Role	Role for other school staff with access to more features than students but fewer features than other staff such as teachers, school administrators, headteacher and IT administrators. They have access to: <ul style="list-style-type: none"> • Staff Portal Microservice • Staff files and folders however some private and confidential files will be restricted to certain members of staff and access may be granted or denied depending on their jobs. • Access to more online content than students however illegal, extremely inappropriate and malicious content and malware will still be blocked.
Load Balancers	Load Balancer	Description
	External Load Balancer	Redirects external internet traffic to the school website for unauthenticated members of the public and to the internal school IT system when accessing the school's internal portal externally as an authenticated user.
	Internal Load Balancer	Redirects network traffic to the school's internal portal microservices and to the School IT System Load Balancer.
	School IT System Load Balancer	Redirects network traffic to the different IT system software containers.
Network Gateways	Gateways from AWS platform to school intranet and existing on-site IT infrastructure and to the internet.	
Elastic Cloud Compute (EC2) instances	Three instances for development, testing, deployment and release of school portal microservices, website and IT system software as Docker container images.	
Cloud9	Integrated Development Environment for coding, developing, building, deploying and releasing school website, portal and IT system software and using command line interface to interact with other development tools.	
Docker	Containerisation platform to containerise school website, portal microservices and school IT system software applications as images to be committed to AWS Elastic Container Registry.	
CodeCommit	AWS Git repository(s) for website, portal and IT system software development for version control and backups and CI/CD pipelines.	

Elastic Container Registry (ECR)	Container image registry for website, software, and portal container images to be deployed on AWS Elastic Container Services.	
Elastic Container Services (ECS)	Container orchestration service to deploy, manage and scale containers for the school IT system, website and portal.	
Simple Storage Service (S3) Buckets	Object storage used to store the files for the portal and website content.	
Elastic Block Storage (EBS)	Store IT system applications and software files, databases staff files and student files due to having faster access and higher performance than S3 buckets as applications, databases, student and staff files are in constant use.	
AWS S3 Glacier	Backup and redundant storage for portal, website and application/software files, student files, staff files and school database for disaster proofing.	
AWS Relational Database Service (RDS)	School's database containing student and staff records, other school records, student grades, behavioural reports, financial records, lessons as different tables in one database. Will likely be split into multiple databases in the future for extra security and data protection. Database uses SQL however containers that access the database will use SQL embedded in their own programming languages (Python, C++, C, C#, Java, JavaScript, Swift, PHP, Kotlin) for execution so the users can use a graphical user interface instead of having to enter SQL directly into the database.	
Cloud Management and Governance	Component	Description
	AWS Cloud Formation	Set up and configure AWS resources, infrastructure management.
	AWS CloudWatch	Monitor AWS school IT infrastructure and obtain logs of activity on the IT system. Used for diagnostics and troubleshooting, detect and obtain evidence of misuse of the IT system such as unauthorized access, undesired changes by students and other users, cyberbullying and trolling using the school IT system's applications and services and other forms of misuse.
	Config	Configuration settings for the AWS school IT system.
	Management Console	Management and settings for school IT system.
	Systems Manager Incident Manager	Manage incidents such as errors, cyberattacks, disasters, misuse.

	Patch Manager	Install updates/patches to school IT system containers, website and portal containers, school software hosted on AWS, other AWS components and AWS infrastructure.
School Internal Portals	Access school IT system applications, services, resources and files internally and externally. These portals are deployed as containers.	
	Portal Microservice	Description
	School Internal Portal Student Microservice	Accessible to secondary school and sixth form students. Access to software and services available to students and student files. Most restricted portal microservice with no administrator privileges.
	School Internal Portal Staff Microservice	Accessible to school staff with access to everything included in the student microservice. Staff only applications, services and systems are available in this microservice depending on IAM roles. Staff and student files are accessible in this microservice. Fewer restrictions and partial administrator privileges.
	School Internal Portal IT Administrator Microservice	Access to everything included in the staff and student microservices. Access to IT and AWS administration software and services. Access to all files. Very few restrictions with full administrator privileges depending on IAM roles.
School Website	Container hosting school website available to the public outside of school with no authentication.	
School IT System Application Containers	Containers that host different applications within the school IT system to perform various tasks.	
	Container	Description
	School Register and Attendance Container	Take class registers and record student attendance.
	Student Records Management System Container	Access and manage student records (create, read, update, delete (CRUD)) from school database(s).
	HR and Staff Management Containers	Human Resources Management Software for school staff.
	Educational Software Containers	Containers for educational software for use in class by teachers, students and for homework. Includes educational software for Maths, English, Science, Technology, Computing, Information Technology, Foreign Languages,

		History, Geography, PSHE, Physical Education, Religious Studies, Business Studies, Music, Art, Drama and other curriculum subjects.
	IT Administration Software Containers	Manage school IT system and AWS. Includes management and governance applications. Patch/Update Manager, cybersecurity software, diagnostics and troubleshooting, technical support, backups of files and databases, Control Panel and Settings.
	School Administration Software containers	Software for school office staff for school administration.
	Marking, Assessment and Grading Software Containers	Uses Lambda Function to take in classwork, homework, exams and assignments from their submission containers, marks and grades the submitted work and calculates the grades of the submitted work then presents the
	Teacher and Class Timetabling Software and Containers	Used by headteacher and school administrators to timetable lessons and teachers. Teachers can view their timetables.
	Student timetabling software container	Teachers and school administrators can set timetables for students. Students can view their timetable.
	Online Teaching System Container	Software to enable online classes and resources to educational resources if class cannot be attended on school premises.
	File Management System Container	Manage school files (student, staff, system and applications) access to specific files depends on IAM roles and authentication for data protection.
	Communication System Container	Communication system for staff and students. Communication by message, email, video conferencing, phone calls and file transfer and attachments. IAM roles determine level of access to communication system, access to features and contacts. CloudWatch used to prevent and record misuse of system such as cyberbullying and trolling.
	Staff Payroll Management System Container	Manage staff payroll by headteacher and Human Resources department.

	School Accounting and Finance System Container	Manage school finances and budget by school administrators and headteacher.
	Task and Project Management System Container	Manage school projects and the tasks associated with them. Includes class related projects and non-class related projects. Accessible to school staff.
	Assignment, Coursework and Exam Submission System Container	Students submit coursework, assignments and exams under exam conditions (if exam), checks for plagiarism, AI generated content, inappropriate content and obvious cheating, sends submitted work to Lambda function for marking and grading, sends submitted work to exam board. Results are stored on student records database.
	Classwork Submission Container	Students submit classwork through this container for marking and grading (uses lambda function), checks for plagiarism, AI generated content and inappropriate content. Classwork is then submitted to teacher. Homework grades and reports stored on student records database.
	Homework Submission Container	Students submit homework through this container for marking and grading (uses lambda function), checks for plagiarism, AI generated content and inappropriate content. Homework is then submitted to teacher. Homework grades and reports stored on student records database.
	Class Presentation Software Containers	Presentation software for teachers and headteachers to present slideshows in class, lectures and assembly.
	School Trip Planner Software	Planning software for school trips.
	Student Management System container	Manage matters regarding students.
Lambda Function	Obtain work from submission containers, mark and grade the work and send results to Marking, Grading and Assessment containers.	

Findings and Recommendations

Findings

Findings from the literature review have concluded that the school would benefit from an Amazon Web Services (AWS) cloud-based IT system and infrastructure to upgrade its outdated IT infrastructure. Research was conducted into using cloud computing in schools in the UK and other schools are using cloud computing solutions in the UK, USA and other countries. Cloud computing solutions for schools are recommended by the UK government (Department for Education) (Department for Education, 2019). The economic benefits of cloud computing in schools includes eliminating the need to purchase expensive new IT equipment and servers, using less energy consuming IT equipment and cheaper cloud-only devices, requiring fewer IT staff, and using pay-as-you-go and subscription services instead of expensive software licensing fees.

Efficiency benefits of a cloud-based IT system includes using automation to save students', staff and teachers' time on tedious tasks and more time on productivity such as in school administration, management and human resources departments. This includes using collaboration tools for communication, sharing files, databases, lesson content, documents and online classes between staff and students. Physical textbooks and library books can be replaced with e-books to prevent damage, vandalism, loss and theft. Cloud computing solutions allow schools to use the latest educational software and easily facilitate remote and online learning. School IT software is automatically updated and managed using cloud services such as AWS Patch Manager. Up-to-date software improves cybersecurity and provides the latest features and fixes bugs.

Schools use cloud computing for disaster recovery solutions by backing up files, data, databases and software to the cloud. Data already stored on the cloud such as in AWS S3 Buckets can automatically be backed up to AWS S3 Glacier. This will help the school in the event of data loss due to hardware or software failures, malicious attacks and ransomware attacks. Cloud computing benefits schools by providing enhanced cybersecurity using firewalls, Identity Access Management (IAM) roles, hardened container images and operating systems, and security groups which is important for data protection. The use of CI/CD pipelines and DevOps tools on cloud computing platforms makes the development of specialist school, educational and assistive software more streamlined and quicker. Artificial intelligence and machine learning can assess assignments and exams and check for plagiarism and AI-generated content used for cheating and grade the assignments and provide feedback to students and teachers. Machine learning can also analyse data patterns to give students a more personalised learning environment. Cloud computing solutions can provide assistive technologies to students with special needs to bring them to their full potential.

The literature review states that there are some considerations that the school must consider including the speed of their internet connection, financial feasibility of

creating a cloud-based IT system, are any of the school's IT systems already cloud-based, the quality of the school's internal intranet, will the staff and students adopt the new IT system, and how many IT systems the school wants to put in the cloud.

There are also concerns regarding cloud computing in schools including reliability and downtime, internet speed, privacy, security and data protection, dependence on service providers, complexity of managing multiple platforms and data and resource control limitations.

Amazon Web Services (AWS) provides several services for cloud computing systems that are already implemented in other schools. The reasons why schools choose AWS is that it is cost effective, has a high standard of privacy, security and data protection which is important due to the sensitive data schools' use. AWS services are elastic and scalable and can adjust to the school's IT demands in real-time preventing system slowdowns and overloads unlike a traditional school IT system. Some services include remote and virtual learning, planning and educational performance tools, student and staff management systems, ransomware mitigation, learning management systems, school administrative systems, data and database management products, library management software, student analytics and infrastructure modernisation.

From the Cloud Readiness Assessment conducted on Amazon Web Services (AWS) for the school and its IT system which consisted of a series of questionnaires on different aspects of the school's cloud readiness that included business, people, governance, platform, security and operations, the school would benefit from a cloud-based IT system. A summary of the findings from the CRA assessment will be included here.

Business:

From a business perspective the school should adopt a cloud based IT system to reduce technical debt from outdated on-site IT infrastructure, use automated tools to assist with migrating school's digital assets (files, data, databases, software, IT infrastructure) to the cloud, use agile and DevOps methodologies with CI/CD pipelines to streamline development, deployment and orchestration of cloud software for the school's IT systems and use data analytics, data science artificial intelligence and machine learning to assist with reports, grading and personalised learning environments for students by analysing data. This must comply with the Data Protection Act 2018.

People:

From a people's perspective, the CRA report states that the school staff need training on how to use the cloud-based school IT system and IT staff need training for its development, orchestration, management and maintenance. Furthermore, the school needs to adopt a modernised transformational leadership to allow staff to transform t

using cloud services. The school will need to adopt risk management plans to mitigate risks associated with the cloud transformation project and adopt a top-down approach.

Governance:

The school must adopt risk management plans to mitigate risks associated with cloud computing such as privacy, security and data protection, child protection and online risks such as harmful content and how to respond to these risks. The school needs to move its most critical applications to the cloud first then move less critical applications to the cloud. The school must assign data governance roles including data owners, stewards and custodians. The cloud solution must comply with the Data Protection Act 2018.

Platform:

A well architected cloud environment will accelerate its implementation, reduce associated risks, cost, complexity and technical debt. The school can set up guardrails for authentication, security, networking, logging and monitoring. Cloud services can be created to automate school authentication processes and assessment monitoring processes. Containers can be used for school applications for optimised resource allocation and scaling and as independent microservices. The school should set up connectivity between the premises and the cloud to allow a hybrid cloud that integrates the on-site infrastructure with the AWS cloud platform. The school needs to start with a minimum viable product by migrating the most critical applications to the cloud first. The cloud developers should test cloud software as early as possible the commit to the Git repository to prevent bugs, vulnerabilities and technical debt that will compromise the cloud-based IT system.

Security:

In a school, security must be paramount due to the sensitive and confidential data that a school IT system contains therefore must comply with the Data Protection Act 2018, the Computer Misuse Act 1990, the Online Safety Act 2023 and GDPR therefore security measures must be implemented such as IAM roles, firewalls, cybersecurity software and security groups. Cloud storage must be encrypted to prevent unauthorized access. The IAM user roles will prevent unauthorized access to restricted data and prevent unauthorized changes to the AWS cloud IT infrastructure for the school and restricted applications. School should use monitoring software to detect threats and incidents. The school needs to use private clouds to connect to private components to prevent external unauthorized access and implement zero trust policies. Machine learning can be leveraged to detect the latest threats. Use cloud services to automate security tasks. Use disaster proofing and backups in the event of a cyber-attack or security incident that affects files/data/databases.

Operations:

The school should utilise AWS tools that use machine learning and artificial intelligence to monitor AWS system resources for diagnostics, troubleshooting, error detection, cybersecurity threat detection, to detect abuse and misuse of the school's AWS IT system and display the data generated on a centralised single dashboard for a unified view of the school's IT system and performance. The school can use the cloud to back up data using AWS S3 Glacier for disaster proofing in accordance with the disaster recovery plan and can also use AWS S3 Buckets and AWS Elastic Block Store (EBS) for the main file storage. AWS tools such as Patch Manager can be used to keep AWS cloud software updated, applying critical updates immediately and less critical updates when school is closed to reduce disruption. A single console can be used to consolidate and manage all the school's IT infrastructure into a single console.

Full Cloud Readiness Assessment is available here: <https://cloud-computing-diagrams.onrender.com/static/CRA-Report.pdf>

Recommendations

AWS Diagram available here: <https://cloud-computing-diagrams.onrender.com/>

AWS Diagram also available here: <https://cloud-computing-diagrams.onrender.com/awsarchitecturediagramhtml>

From the research and AWS Cloud Readiness Assessment, I would recommend that a cloud-based IT infrastructure system using Amazon Web Services (AWS) would benefit the school and be a solution for its outdated IT infrastructure for the following reasons:

- Save money by not having to spend a large amount of money on upgrading the school's on premises IT infrastructure.
- Upgrade the school's IT infrastructure and use the latest technologies without spending large amounts of money on upgrading the school's on-site IT infrastructure.
- Save money using pay-as-you-go and subscription services instead of paying expensive software licensing fees.
- Disaster proof school data using cloud backups and storage in the event of a disaster such as data loss, a cyberattack especially ransomware and damage to on-site IT infrastructure, hardware or software failures.
- AWS and other cloud platforms provide a wide range of educational and administrative tools for schools and educational institutions.
- Resources (files, data, software, communications, teaching materials, learning environments, books and other school resources) are accessible from anywhere, any time and any internet connected device.

- Cloud computing leverages software that automates IT and school administration tasks that makes IT and school administration more efficient, increases productivity and reduces tedious tasks.
- Easy to facilitate online, virtual and remote learning if the school premises are closed due to an emergency or if a student or teacher is unable to get to the school premises.
- IT administrators can manage the school IT systems remotely when the school is closed and if they are unable to arrive at the school premises or due to technical or operational reasons.
- School IT system using cloud solutions can be more secure than on site premises incorporating firewalls, IAM roles, hardened system images and operating systems, backups, security group and security software.
- Cloud systems can provide assistive software to all students helping students with special needs and disabilities and is deployable rapidly using CI/CD pipelines.

An AWS architectural diagram has been created for the recommended school's IT infrastructure cloud solution. Amazon Web Services (AWS) has been chosen because it has a high regard for customer privacy and security therefore is good for a school's IT system that holds large amounts of sensitive and confidential information and content generated by children that must be protected in accordance with the Data Protection Act 2018, Computer Misuse Act 1990, Online Safety Act 2023 and GDPR. AWS is also recommended because of the vast number of AWS tools available, AWS being the most established cloud computing platform and because AWS already provides several educational tools for schools and is already used in other schools.

Amazon Web Services (AWS) Architecture Diagram for School I.T. System. Authour: S275931

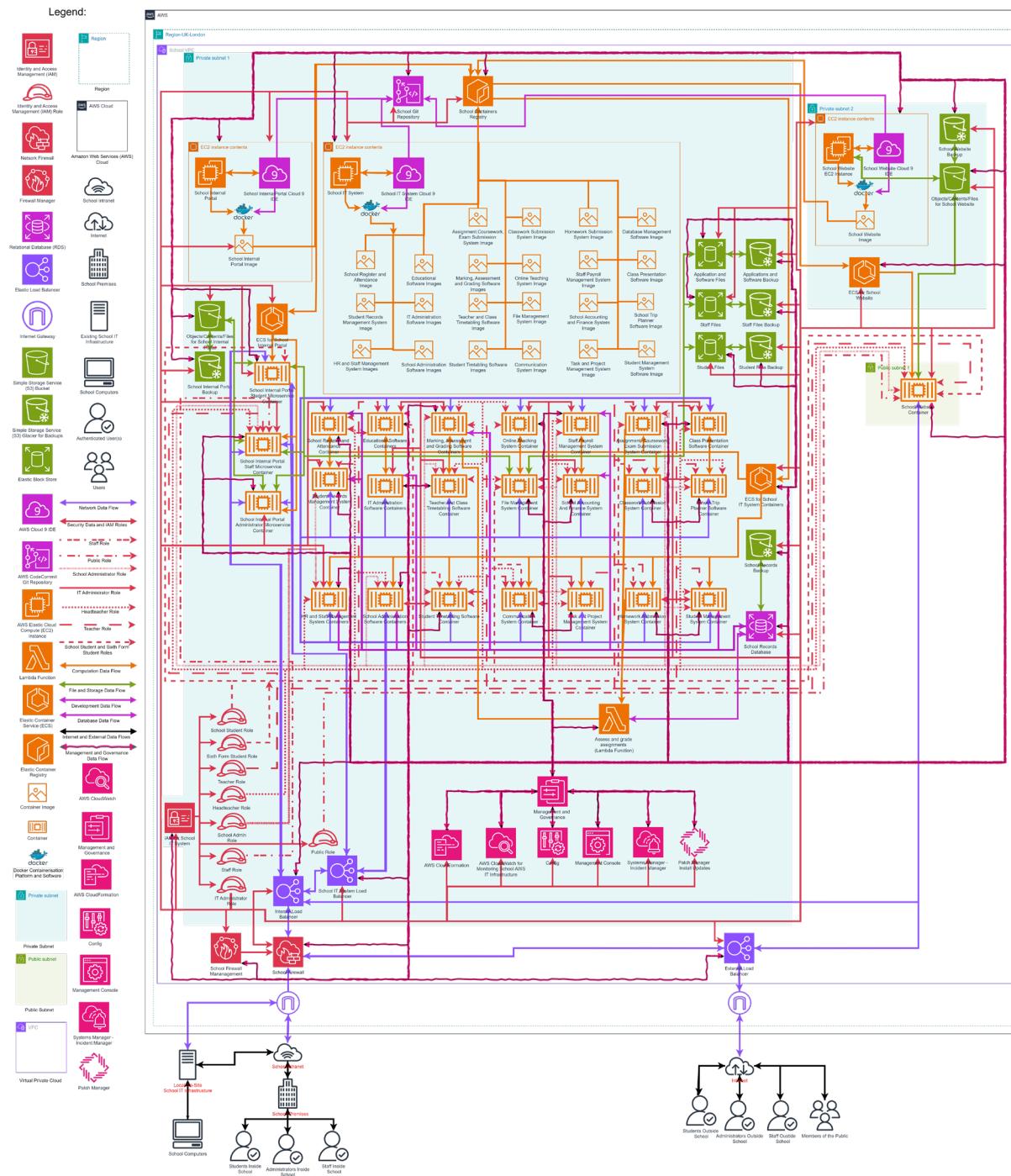


Figure 2 - Amazon Web Services architecture diagram for the school IT system. Zoom in to view content.

For full recommendations, see [Appendix E: Cloud Recommendations](#).

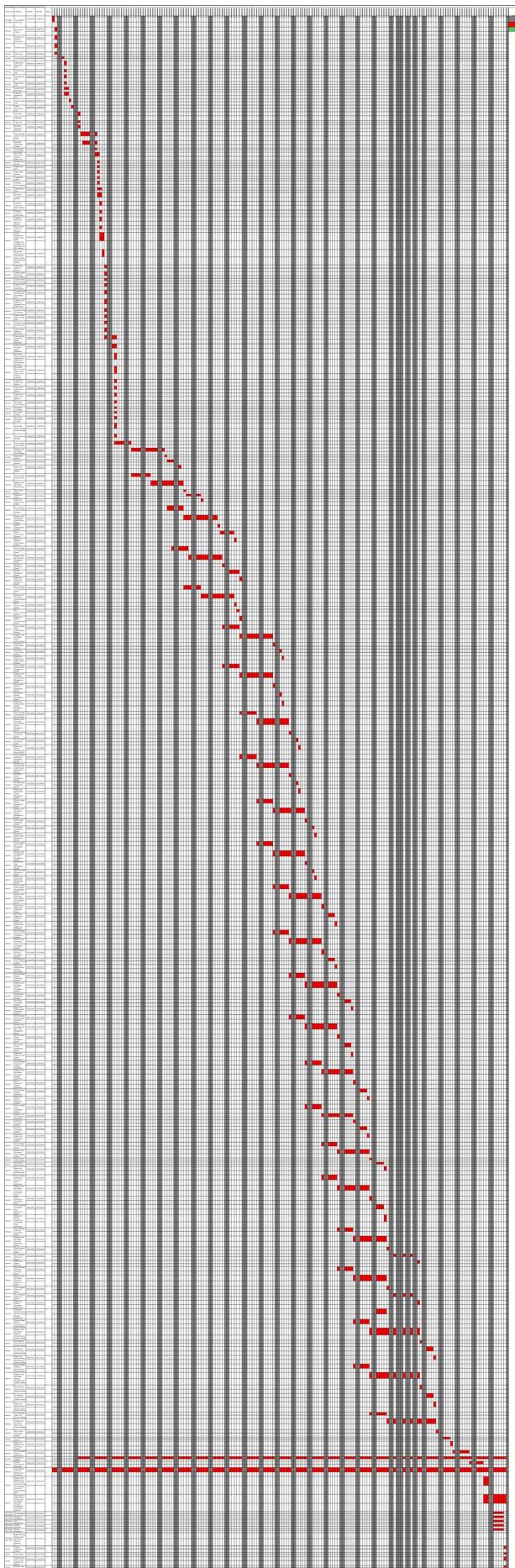
Road plan for Implementation

A Gantt Chart has been created to provide a timeline to implement the school's cloud-based IT system on Amazon Web Services over a six-month period starting on the first of August 2024 and ending on 8th February 2025. The red timelines on the Gantt Chart spreadsheet is the planned timeline for implementation and the green timeline (not yet added as this is a proposal) is the actual timeline of this project.

Full Gantt Chart can be viewed here: <https://cloud-computing-diagrams.onrender.com/static/School%20Cloud%20Computing%20System%20Project%20Gantt%20Chart.html>

Downloadable Gantt Chart as Excel Spreadsheet available here: <https://cloud-computing-diagrams.onrender.com/ganttchartdownload>

Image of Gantt Chart (zoom in to view content):



Conclusion

The key takeaway findings of this report is that the school would benefit from a cloud-based IT system and infrastructure to replace its outdated IT infrastructure that is slow, unreliable and obsolete with a new traditional on-site school IT system due to benefits including:

- Lower costs
- Constantly upgradable without expensive on-site hardware upgrades.
- Lower maintenance as the IT system is maintained remotely by Amazon Web Services instead of school IT staff.
- Saves time in terms of setup, upgrades, maintenance, security and updates.
- More efficient software for school administration, teaching and learning.
- Disaster proofing for data loss caused by hardware and software failures and cyberattacks by backing up data to S3 Glacier backups.
- Wide variety of educational software is available
- Facilitates option for remote learning.
- High degree of cybersecurity on AWS.

Research has revealed that other schools are using cloud computing systems for the same reasons due to cost savings due to the limitations of school budgets and government funding while still being able to use the latest teaching, learning and administration technologies. However, there are some points the school must consider before adopting a cloud-based IT system such as internet speed (full fibre dedicated leased line is required), on-site networking infrastructure (routers, switches, hubs, wireless access points, network cables) being up to standard, data protection and privacy and local regulations and compatibility.

Limitations of this study included not having time to use all three platforms mentioned in the literature review, not creating the actual school's IT system on AWS Academy as practise thus limiting my understanding of all features included my inexperience of using AWS is a further limitation and therefore could be errors in my AWS architectural diagram. Another limitation was that using AWS cost estimator was not included in this assignment and due to the complexity of AWS cost estimator, there could be inaccuracies in how much money my proposed IT system save the school.

Furthermore, the school is a fictional secondary school in the UK – not a real UK school.

Further improvements to the study would be to include containers for assistive technologies and a Library Book system in the AWS architectural diagram and include them in the Gantt Chart for implementation so the school's cloud-based IT system is inclusive for students with special needs. I learned about cloud-based assistive technologies and library management systems when writing the literature review after creating the AWS architectural diagram. These will be included in future assessments.

References

- Amazon Web Services (2024) *Admissions & Financial Aid Processing*. Available at: <https://aws.amazon.com/solutions/education/admissions-and-financial-aid-processing/> (Accessed 19 07 2024).
- Amazon Web Services (2024) *Analytics*. Available at: <https://aws.amazon.com/solutions/education/analytics/> (Accessed 19 07 2024).
- Amazon Web Services (2024) *AWS Cloud Adoption Framework (AWS CAF)*. Available at: <https://aws.amazon.com/cloud-adoption-framework/> (Accessed 10 07 2024).
- Amazon Web Services (2024) *AWS Cloud for K12*. Available at: <https://aws.amazon.com/education/K12-primary-ed/> (Accessed 19 07 2024).
- Amazon Web Services (2024) *Contact Center*. Available at: <https://aws.amazon.com/solutions/education/contact-center-k12/> (Accessed 19 07 2024).
- Amazon Web Services (2024) *Core Administrative Systems*. Available at: <https://aws.amazon.com/solutions/education/core-administrative-systems/> (Accessed 19 07 2024).
- Amazon Web Services (2024) *Data Management*. Available at: <https://aws.amazon.com/solutions/education/data-management/> (Accessed 19 07 2024).
- Amazon Web Services (2024) *Data Modernization*. Available at: <https://aws.amazon.com/solutions/education/data-modernization-k12/> (Accessed 19 07 2024).
- Amazon Web Services (2024) *Digital Preservation*. Available at: <https://aws.amazon.com/solutions/education/digital-preservation/> (Accessed 19 07 2024).
- Amazon Web Services (2024) *Identity & Access Management*. Available at: <https://aws.amazon.com/solutions/education/identity-and-access-management/> (Accessed 19 07 2024).

Amazon Web Services (2024) *Infrastructure Modernization*.

Available at: <https://aws.amazon.com/solutions/education/infrastructure-modernization/>

(Accessed 19 07 2024).

Amazon Web Services (2024) *Learning Management System*.

Available at: <https://aws.amazon.com/solutions/education/learning-management-system/>

(Accessed 19 07 2024).

Amazon Web Services (2024) *Library Catalog Management*.

Available at: <https://aws.amazon.com/solutions/education/library-catalog-management/>

(Accessed 19 07 2024).

Amazon Web Services (2024) *Planning & Performance*.

Available at: <https://aws.amazon.com/solutions/education/planning-performance/>

(Accessed 19 07 2024).

Amazon Web Services (2024) *Ransomware Mitigation*.

Available at: <https://aws.amazon.com/solutions/education/ransomware-mitigation-k12/>

(Accessed 19 07 2024).

Amazon Web Services (2024) *Remote & Virtual Learning*.

Available at: <https://aws.amazon.com/solutions/education/remote-virtual-learning/>

(Accessed 19 07 2024).

Amazon Web Services (2024) *Security, Risk, & Compliance*.

Available at: <https://aws.amazon.com/solutions/education/security-risk-and-compliance/>

(Accessed 19 07 2024).

Amazon Web Services (2024) *Student Analytics*.

Available at: <https://aws.amazon.com/solutions/education/student-analytics/>

(Accessed 19 07 2024).

Amazon Web Services (2024) *Student Communications*.

Available at: <https://aws.amazon.com/solutions/education/student-communications/>

(Accessed 19 07 2024).

Amazon Web Services (2024) *Student Management*.

Available at: <https://aws.amazon.com/solutions/education/student-management/>

(Accessed 19 07 2024).

Amazon Web Services (2024) *Virtual Proctoring*.

Available at: <https://aws.amazon.com/solutions/education/virtual-proctoring/>
(Accessed 19 07 2024).

Coursera (2024) *What's the Difference Between AWS vs. Azure vs. Google Cloud?*.

Available at: <https://www.coursera.org/articles/aws-vs-azure-vs-google-cloud>
(Accessed 11 07 2024).

Department for Education (2019) *Moving your school to the cloud*.

Available at: <https://www.gov.uk/government/publications/moving-your-school-to-the-cloud/moving-your-school-to-the-cloud>
(Accessed 10 07 2024).

Dhaduk, H. (2022) *AWS vs. Azure vs. GCP: A Complete Comparison Guide*.

Available at: <https://www.simform.com/blog/aws-vs-azure-vs-gcp/>
(Accessed 11 07 2024).

HubVela (2023) *Advantages and Disadvantages of Cloud Computing in Education*.

Available at: <https://hubvela.com/hub/technology/advantages-disadvantages-cloud-computing/education/>
(Accessed 10 07 2024).

Jones, C. (2022) *9 Benefits of AWS for Students and Education*.

Available at: <https://redriver.com/aws/aws-for-students-and-education>
(Accessed 11 07 2024).

Morris, A. (2023) *Cloud Computing In School And Its Benefits*.

Available at: <https://blog.teamsatchel.com/cloud-computing-in-schools-and-its-benefits>
(Accessed 10 07 2024).

Roman Ceresnak, P. (2024) *AWS for Education: Enhancing Learning through Cloud Technology*.

Available at: <https://medium.com/codex/aws-for-education-enhancing-learning-through-cloud-technology-df62d96c93ec>
(Accessed 11 07 2024).

Signapse (2023) *Breaking Barriers with our AI Sign Language Translator*.

Available at: <https://www.signapse.ai/>
(Accessed 11 07 2024).

Appendix

Appendix A: Benefits of using Cloud Based Technologies for School IT Systems

There are several benefits of using Cloud Based Technologies for a school IT system that include:

- Economic benefits – schools often have tight budgets therefore saving money is crucial:
 - Lower license costs by using free cloud applications such as free office software and communication platforms instead of traditional expensive proprietary software (Department for Education, 2019).
 - No electricity used powering on site servers resulted in cheaper electricity bills for the school (Department for Education, 2019).
 - Save money by not having to purchase expensive on-site servers and related infrastructure. Cheaper hardware can be used on site (Department for Education, 2019).
 - Cheaper cloud only devices (desktop computers, laptops, tablets, smartphones) access cloud applications through a web browser and do not require as expensive/high-end hardware as their traditional counterparts that run software locally (Department for Education, 2019).
 - Cloud only devices need to be replaced less frequently and extend lifespan of older devices (Department for Education, 2019).
 - Reduced need to replace old servers (Department for Education, 2019).
 - Uses software-as-a-service, platform-as-a-service and infrastructure-as-a-service with more predictable subscriptions (Department for Education, 2019).
 - Save money through pay-as-you-go services (Department for Education, 2019).
 - Reduced data storage costs (HubVela, 2023).
- Efficiency benefits – saving teachers', students' and staff time:
 - Use school teaching, learning, administration an IT system software on the go on any internet connected device (Department for Education, 2019).
 - Improved collaboration between staff and students including sharing files, documents, databases, lesson content, plans and communication (Department for Education, 2019).
 - More efficient and easier to use curriculum resources and conduct research (Department for Education, 2019).

- Access data and school applications more quickly at any location, on any device and with faster login times (Department for Education, 2019).
 - Cloud computing allows students and staff to access learning materials, software, teaching materials and tools, administration tools, library e-books/e-textbooks on any device, any time and any location (HubVela, 2023).
 - Replace physical textbooks and library books with e-books and paper-based classwork with paperless options saving money on paper, pens and pencils. E-books save money as they tend to be cheaper than paper books, cheaper to replace when curriculum is updated, and e-books cannot get damaged, destroyed, defaced, vandalised, lost or stolen by students in the same way paper textbooks can be (HubVela, 2023).
 - Improved collaborative learning, group work and communication – cloud platforms host communication and collaboration tools to allow students, staff and teachers to work collaboratively on projects, assignments, classwork, lessons and school administration (HubVela, 2023).
 - Reduce tedious work in the school's administration, human resources and management departments by automating such work so staff in these departments spend more time productively (HubVela, 2023).
 - Easy to facilitate remote learning and online classes – Cloud computing is essential for hosting software for online classes and remote learning including video conferencing, sharing teaching and learning materials, classwork and homework. This essential in the event of the school having to close during term time due to an emergency such as COVID-19 or other pandemic lockdowns, problems with the school building or premises, teachers being unwell, severe weather and travel disruption preventing students from attending school (HubVela, 2023).
- Effectiveness:
 - Reduce the workload on school IT administrators and technicians – Applications are automatically updated and managed (Department for Education, 2019).
 - Disaster recovery and backup options reducing the risk of data loss (Department for Education, 2019).
 - Enhanced data and storage management (HubVela, 2023).
 - Increased Cybersecurity – Cloud computing is more secure than traditional school IT infrastructure, incorporating firewalls, Identity and Access Management roles, Security Groups, Hardened operating systems, containerisation and cybersecurity software protecting student and staff data and files and reduce the risk of a cyberattack or malware. This is especially important due to the sensitive nature of data that schools handle (Morris, 2023).

- Learning and Teaching – more effective solution for personalised learning:
 - Teachers can tailor learning experiences and environments to individual students' needs for more effective education and more successful outcomes (HubVela, 2023).
 - Use cloud computing such as Artificial Intelligence (AI) and Machine Learning (ML) tools to analyse student data, learning patterns, grades, assignments, classwork and homework to inform the teachers with recommendations on how to cater for each student to bring them to their full potential by catering for their learning style, pace and ability (HubVela, 2023).
 - Cloud based school IT systems allow teachers to provide feedback to their students on how to improve their classwork, grades and learning (HubVela, 2023).
 - Access to a wider range of learning resources (textbooks, library books, learning materials, teaching materials and software) that is available in a typical school classroom/library/IT system (HubVela, 2023).
 - Personalised learning is more flexible to students (HubVela, 2023).
- Students with Special Needs – Cloud computing makes education more accessible to students with special needs:
 - Cloud-based school IT systems make sure disabled students have access to learning resources, using assistive technologies that allow them to have greater independence, opportunities and mobility than previously (HubVela, 2023).
 - Cloud computing applications can be bundled with assistive technologies such as magnifiers, high contrast, sticky keys, screen readers, learning disability software, text-to-speech engines and speech recognition, closed-captions, AI-generated sign language in videos and audio (Signapse, 2023), integration with induction loops to assist students with a range of disabilities as well as those without disabilities (HubVela, 2023).
 - Assistive software can be deployed within days instead of weeks or months using a cloud-based IT system leveraging DevOps and CI/CD pipelines as well as no need for disabled students to visit a specialist education centre, barriers between disabled students and their studies, graduation and success are broken down (HubVela, 2023).

Appendix B: Considerations, Drawbacks and Using AWS for School Cloud Computing Platforms

Considerations for using Cloud Based Technologies for School IT Systems

There are several considerations the school to consider before implementing the cloud-based IT system/infrastructure. These include (Department for Education, 2019):

- What cloud-based systems is the school already using.
- How much money would the school save compared to upgrading their existing IT systems using traditional means.
- Financial feasibility of a cloud-based IT system.
- Do school staff, students, teachers, parents already use unofficial cloud services instead of the existing IT infrastructure?
- What are the benefits and drawbacks of transitioning the school to a cloud-based IT system? Consider cost, security, time, online safety, data protection, privacy, compatibility, positive and negative impacts on students, teachers, staff, parents and the school itself.
- How to integrate the new cloud system with the old on-site systems?
- Will the school use the cloud-based IT system to its full potential?
- Will the staff and students accept the changes to the IT system?
- How many functions can be put in the cloud?
- Is the school's internet connection fast enough to use cloud technologies? Full fibre optic (FTTP) connection is required.
- Is the school's internal network (intranet) adequate? Wired connections (ethernet, fibre optic, USB, Coaxial cable, DSL) and wireless connections (Wi-Fi, 4G/5G mobile data, Bluetooth, Mesh Networks, Zigbee) are required to support a range of devices to access the cloud. Is the school networking equipment (routers, switches, hubs, wireless access points, servers) fast enough to handle vast amounts of data for a cloud-based infrastructure (Department for Education, 2019)?

Disadvantages of using Cloud Based Technologies for School IT Systems

There are several disadvantages of cloud-based school IT systems that the school must consider including:

- Reliability and Downtime – Cloud computing relies on a fast and reliable internet connection because the actual computation and school IT systems are being hosted on a remote server at a data centre instead of on school premises. Server/Data Centre downtime and loss of internet connection will bring the school's IT systems to a grinding halt with severe disruption to teaching, learning, IT and school administration. School should consider redundant systems, an

ultrafast reliable internet connection and a reputable cloud platform to mitigate this (HubVela, 2023).

- Security and Privacy – Schools have a lot of confidential data including personal and sensitive information on students, staff, financial and operational information, login credentials, files created by students and staff must comply with strict data protection policies. The risk of data breaches and privacy violations increases when the data is stored outside of school premises. Failure to comply with data protection laws can result in legal consequences for the school and its staff responsible (HubVela, 2023).
- Dependence on Service Providers – Schools will require constant internet access to use a cloud-based IT system which requires an Internet Service Provider (ISP) – Loss of internet connection or poor bandwidth will make the cloud-based IT infrastructure unusable, detracting from learning. Furthermore, cloud computing for schools uses a single vendor and is difficult to switch vendors due to proprietary components and predatory vendor lock-in. Unreputable cloud providers or a poorly designed cloud system can put data at risk and risk of cyberattacks and malware (HubVela, 2023).
- Risk of Data Loss and Breaches – Increased risk of data loss and data breaches especially of sensitive data on cloud platforms due to the server being in a remote location with data sent over the internet between the school and the data centre and due to the cloud-based infrastructure being hosted by a third-party. Cybercriminals are more likely to attack large data centres compared to individual schools resulting in multiple organisations being attacked (HubVela, 2023).
- Managing multiple platforms is complex. School staff, students, IT administrators and parents/carers need to be more computer literate when using cloud-based school technologies, especially when using multiple platforms for different services as they require a deep understanding of how these different platforms interact with each other (HubVela, 2023).
- Data and resource control limitations – Cloud data centres and servers are owned, monitored and managed by the cloud service provider meaning that the school IT administrators and school management have little control over what happens to the data once it is uploaded to the cloud as they do not have access to the physical servers therefore cannot manage them in the same way as an on-premises server. Cloud providers enforce End-User License Agreements (EULA) and management policies that may restrict the school's control even further (HubVela, 2023).
- Learning Curve – IT administrators and technicians will need training on how to set up, orchestrate, manage and use the cloud-based school IT system/infrastructure as operating it is different to operating traditional IT

infrastructure. Teachers, parents, students and other school staff will need training and learn how to use the cloud-based systems. This can be difficult if the user(s) are computer illiterate or disadvantaged by the digital divide (HubVela, 2023).

Using Amazon Web Services for School IT Systems

There are several reasons to use Amazon Web Services (AWS) as the cloud computing platform for cloud-based IT systems in schools including:

- Elasticity and Scalability – Unlike a traditional school IT system, a cloud-based school IT system using AWS is elastic and scalable meaning that the amount of computing resources for the school IT system is dynamically adjustable on demand. For example, the IT system is scaled up (allocating more resources) during times of heavy use such as exam season or enrolment to accommodate for more students and staff using the system simultaneously and scaled down (allocating fewer resources) during times of light use such as the school holidays and weekends to save money (Roman Ceresnak, 2024).
- Data protection, cybersecurity and privacy – AWS provides a variety of data protection, security and privacy features such as encryption, Identity Access Management (IAM) roles, Firewalls, Security Groups, hardened container images, backup and disaster recovery and cybersecurity services. This especially important for a school because of the confidential, sensitive and personal data a school uses, to protect children from online harm through the school's IT systems, prevent malware and cyberattacks on the school IT systems and to prevent unauthorised tampering with the school IT systems (Roman Ceresnak, 2024).
- AWS is cost effective – AWS eliminates the high costs associated with purchasing, running, maintaining and upgrading traditional on-site school IT infrastructure. No more expensive hardware purchases and fewer IT staff required. Pay-as-you-go pricing allows for further cost savings on infrastructure and avoid paying expensive software licenses (Roman Ceresnak, 2024).
- AWS can help students learn how to create, orchestrate and manage cloud computing systems too during IT and computing classes. This can also help students get AWS certifications as well as contributing to their regular National Curriculum, GCSE, A-Levels, T-Levels, B-Tecs, NVQs in IT, Computing and Computer Science. AWS Academy and AWS Educate could be used for this (Jones, 2022).
- Learning Environment – AWS uses virtualisation and isolation therefore students can learn IT, computing and computer science in more intuitive ways as the virtualisation allows students to develop apps and websites, orchestrate infrastructure, be a system administrator, and perform other computing tasks

without the risk of damaging the school's actual IT infrastructure therefore allowing students to learn about computing aspects that they would not be able to do on a traditional school IT system. The virtual machines are backed up in the event of a student damaging their own virtual environment (Jones, 2022).

- Career opportunities – AWS education can open cloud computing career opportunities to students (Jones, 2022).
- AWS can host educational apps for students to use for learning, classwork, homework, assignments and study. Teachers can use these educational apps for teaching classes, setting classwork, homework and assignments. These educational apps can also assist with online classes and remote learning. The educational apps can be developed directly on AWS or uploaded to AWS (Jones, 2022).
- AWS provides online portals for students to learn remotely and teachers to teach remotely at any time, any place, on any internet connected device (Jones, 2022).
- AWS virtualisation allows virtual machines to be used instead of physical computers allowing students to do IT and computing work without needing a dedicated computer lab. This also allows students to practice computing skills better by giving students administrator privileges in the isolated virtual machines without the risk of interfering with the school's IT infrastructure including AWS infrastructure if something goes wrong (Jones, 2022).
- AWS provides a variety of tools and customised online infrastructure allowing the school to build its infrastructure on AWS and allow it to be managed by a managed service provider instead of having to manage their own educational apps and resources (Jones, 2022).

Appendix C: AWS Educational Products

Amazon Web Services (AWS) provides a wide and comprehensive range of educational and management products for schools and educational institutions. These AWS tools include cost-effective and scalable computing resources, remote learning, cloud storage, collaboration tools, research tools, services to process data intensive workloads, disaster recovery, enhanced cybersecurity, and access to the latest technologies (Amazon Web Services, 2024). These services include:

- Remote and Virtual Learning – provides teachers and students to learn remotely and flexibly, provides livestreaming of classes and hosts pre-recorded videos of classes accessible by students anytime. Also provides virtual learning content, resources, assignments and progress indicators (Amazon Web Services, 2024).
- Data Modernisation – Allows schools to adopt a more agile approach to innovation and transformation to the cloud and embrace new technologies. AWS is a more cost-effective solution than traditional school servers as traditional school servers are costly to maintain and require specialist staff

which hinders schools from being to adopt new technologies (Amazon Web Services, 2024).

- Planning and Performance – AWS allows schools to leverage artificial intelligence, machine learning, business intelligence, data science, and natural language queries to find the correct data more quickly and easily to make school management more efficient such as student management systems, school bus timetables, student information systems. This will improve productivity of school staff (Amazon Web Services, 2024).
- Student Management – Student management solutions on AWS allows scalable, reliable high-performance services to handle high volumes of variable data on students every day and provides security and data protection through Identity and Access Management (IAM). This data includes student intake, attendance, and assignments, which is accessible to teachers, parents and students (Amazon Web Services, 2024).
- Ransomware Mitigation – AWS ransomware mitigation and disaster recovery provides easy solutions to recover school data affected by a ransomware attack and is updated regularly as cyber threats evolve (Amazon Web Services, 2024).
- Analytics – AWS analytics solutions use artificial intelligence and machine learning to process and analyse data to open insights into students' academic progress and performance and is accessible to students, teachers and parents. Analytics reduces siloed data and increases its visibility and upholds security and governance (Amazon Web Services, 2024).
- Contact Centre – Uses artificial intelligence chatbots to automate the contact process reducing burden on staff and improving communication. This includes phone calls to report absences, emergencies and activity reminders (Amazon Web Services, 2024).
- Learning Management System – Provides a remote and personalised scalable learning environment that is highly secure and accessible. This learning environment is digital and remote and connects assignments, resources and progress indicators with students, parents and teachers (Amazon Web Services, 2024).
- Core Administrative Systems – AWS provides solutions for school administrative solutions that provide a user-friendly experience, leverages disaster recovery to provide resilience to outages on campus, and allows adaption to change in institutional requirements. This supports administrative management for finance, human resources, and academic process administration (Amazon Web Services, 2024).
- Data Management – AWS helps break down data silos to improve efficiency by supporting the collective governance of data assets such as data governance

policy management, integration requirements across decentralised systems and data catalogues (Amazon Web Services, 2024).

- Identity Access Management (IAM) – provides security, data protection and user roles to prevent unauthorised access to restricted data and administrative AWS settings while ensuring 24/7 access to data and the cloud for people who are authorised to access it (Amazon Web Services, 2024).
- Infrastructure Modernisation – AWS allows the use of hybrid cloud computing solutions therefore the school can use its existing IT infrastructure in combination with AWS cloud-based school IT infrastructure. AWS allows disruption caused by migration to the cloud to a minimum. AWS allows schools to maximise investments and reduce costs, time and risks (Amazon Web Services, 2024).
- Security, Risk and Compliance – AWS provides services that provide security, enhanced threat detection and reduce response times reducing risk to cloud-based school IT systems (Amazon Web Services, 2024).
- Admissions and Financial Aid Processing – AWS accelerates admissions and financial offices allowing them to streamline the process of admitting new students to the school every September (and at other times of the year if a pupil changes school) (Amazon Web Services, 2024).
- Student Communications – AWS provides 24/7 bidirectional multimodal communication tools that are personalised for each student (Amazon Web Services, 2024).
- Student Analytics – Provide enrolment and engagement analytics on students and provides insights on student's progress to teachers and administrators (Amazon Web Services, 2024).
- Library Catalogue Management – AWS provides management tools for school libraries to manage books and other library assets for librarians, students and teachers and stores library books and textbooks in e-book form. Artificial intelligence and machine learning makes research using library books more productive (Amazon Web Services, 2024).
- Digital Preservation – Using AWS to store school library books and textbooks preserves them and prevents them from being damaged, vandalised, lost or stolen (Amazon Web Services, 2024).
- Virtual Proctoring – Students can take tests and exams under exam conditions electronically (Amazon Web Services, 2024).

Appendix D: Cloud Readiness Assessment

An AWS cloud readiness assessment has been conducted for the school and their current outdated IT System to assess how beneficial the cloud-based IT system would benefit the school. This assessment includes a series of multiple-choice questions on

Business, People, Governance, Platform, Security and Operations aspects of the school. Due to the school's outdated IT infrastructure and outdated management methods, the school got a low cloud readiness score therefore it would be beneficial to the school to implement a cloud-based IT system in the school. The most important results from the Cloud Readiness Assessment are below (Amazon Web Services, 2024).

Full Cloud Readiness Assessment is available here: <https://cloud-computing-diagrams.onrender.com/static/CRA-Report.pdf>

Business

- The school should explore new cloud-based technologies to overcome technical debt caused by their outdated and substandard IT systems and infrastructure.
- School should prioritize strategic objectives over time to adapt to advances in technology.
- Use automated discovery tools and seven migration strategy to move applications from existing school IT infrastructure to the cloud.
- Consider financial and non-financial benefits of moving school IT system to the cloud (up to date software, faster IT systems with better performance, can be more cost effective than upgrading physical on-site IT infrastructure, better quality of service, automate tedious office tasks, use latest technologies for teaching, better disaster proofing).
- Use agile methodologies to develop and orchestrate the School IT system cloud platform for rapid evolution and to fix mistakes and make changes if requirements change quickly and easily.
- Use data analytics to obtain technical data for diagnostics and troubleshooting, and non-technical data such as, key performance indicators, assignment grades and behavioural reports to track student, teacher and school performance. Data protection must be adhered to.
- Use data science, artificial intelligence and machine learning (if data protection can be adhered to) to analyse data such as assignment grades, behavioural reports, attendance etc. to measure school, teacher and student performance which will be useful during Ofsted inspections and to identify which students need the most support academically, behaviourally and socially.
- The data science must comply with the Data Protection Act 2018 because schools contain a large amount of confidential, sensitive and personal information on students, staff and the school itself. The cloud computing platform must not sell any data from the school as this would result in serious legal and ethical consequences.
- Use CI/CD pipelines for streamlining the development, integration and development of school IT system applications.

People

- Incorporate new behaviours and mindsets that attract, retain and empower staff to continuously improve and innovate on behalf of the students and other staff. Leverage school's heritage and core values to transform digitally to the cloud.
- Reduce excessive bureaucracy and enable rapid decision-making by using agile methodologies, cross-functional teams and rapid experimentation.
- School should embrace transformational leadership.
- School IT administrators need to be trained in cloud fluency, so they can orchestrate, maintain and manage the AWS cloud school IT system as well as develop for it.
- Modernise the school leadership and staff to successfully transform to the cloud.
- Align and mobilise cross-functional cloud leadership.
- Define success at the start of the transition to cloud based IT system.
- Identify key stakeholders, risks, cross-organisational dependencies and barriers for the school transforming to a cloud-based IT system.
- Reassess the school's cloud readiness in the future.
- Develop a change acceleration strategy and roadmap to address risks and leverage strengths consisting of:
 - Risk Management
 - Talent Management
 - Leadership Action Plans
 - Training
 - Communications
- Engage with school leadership (Headteacher, deputy headteachers, governors, IT administrators and other school staff) to increase acceptance of new ways of working, learning new skills and accelerate adoption.
- Determine if the school is still structured to run in a way that still supports the school's desired outcomes.
- Establish a centralised team that can evolve over time to facilitate and enable the school's transition to AWS cloud for their IT infrastructure.
- Compare trade-offs between centralised, decentralised and distributed school leadership structures.
- Set measurable targets, joint goals, and mechanisms for cloud adoption.
- Top-down approach to develop shared values, processes, systems, working styles and skills to drive school outcomes and break down functional silos between school members (teachers, secondary school students, headteacher, governors, school administrators, IT administrators, sixth-form students, parents/carers, other school staff)

- Set measurable targets, joint goals and mechanisms for cloud adoption, create expectations for skill development to generate sustainable change ownership?

Governance

- Frequently validate roadmap with the project sponsors of the school cloud IT system (school leadership/finance team, UK Government (Department for Education)) and escalate issues to senior leadership.
- Use agile methodologies to enable learning from experience and adapt instead of making far-reaching predictions.
- Identify performance metrics.
- Assess and identify risks relating to school IT infrastructure including availability, reliability, security, data protection, child protection, online safety, risks to school reputation, legal and ethical risks and how to respond to these risks.
- Create risk management plan to reduce and manage risks.
- Use cloud-based services to manage risks associated with running a school and infrastructure failure.
- Use cloud to provision and deprovision resources to reduce procurement risks.
- Clarify roles and responsibilities on school IT systems cloud and make sure school leadership, IT administrators and Department for Education (sponsor) have shared understanding of cloud costs.
- Cloud can allow school to evolve to more dynamic forecasting and budgeting process and detect anomalies with school finances.
- Use consolidated billing to simplify cloud billing.
- Centralise management of cloud software and on-site software licenses to reduce costs.
- Use an accurate and complete inventory of applications.
- Application inventory helps minimise inventory sprawl and assist with cloud transformation.
- Move most critical school IT system applications to cloud first.
- Assign key roles for data governance including data owners, stewards and custodians.
- Make sure all data stored in the cloud complies with the Data Protection Act 2018.

Platform

- The school should develop a well architected cloud environment for its IT system to accelerate its implementation and reduce risk.
- Define blueprints and guardrails to facilitate authentication, networking, security, logging and monitoring.

- Decide what workloads to keep on school premises and which workloads to migrate to the cloud.
- Review hybrid cloud use cases such as backup and disaster recovery to the cloud, cloud bursting, edge computing and distributed data processing.
- Well-designed data architecture to reduce cost, complexity and technical debt.
- Use layered and modular architecture to use the correct tools for each job.
- Use serverless technologies for simplification?
- Use real time data processing and use modern data architecture for movements between data lakes and stores.
- Deploy blueprints and guardrails.
- Integrate AWS cloud school IT system with existing on premises IT system.
- Automate school IT workflows and support security and governance goals.
- Set up connectivity between school's cloud and on premises IT infrastructure.
- Allow users to use their existing credentials for authentication by implementing federation between existing and cloud infrastructure.
- Use centralized logging
- Allow scalability if school population grows.
- Use containers and serverless technologies to optimise resource allocation and automated scaling.
- Decouple school IT applications and build them as independent microservices.
- Automate scaling or use serverless technology.
- Replatforming – move existing applications, containers, databases, files, website to managed cloud services and refactor.
- Adopt DevOps practices including Continuous Integration / Continuous Deployment (CI/CD) pipelines and testing for more efficient cloud development and deployment.
- Start with minimum viable product (school IT cloud with most critical applications) then transition to a CI/CD pipeline later adding more components to the school IT system.
- Encourage school cloud IT system developers to create and run unit tests as early as possible before committing to school Git repository.
- Include staging and production steps in CI/CD pipeline and manually approve production deployments.
- Use multiple deployment strategies such as blue/green, canary, in-place.

Security

- Due to the nature of data being held at the school containing confidential, personal and sensitive information as well as safeguarding files created by children under 18 and staff, strict data protection and security measures are already in place at the school however are currently outdated. Other current but

outdated security measures include the school firewall to block malicious and harmful online content, the antivirus to stop malware and user roles to stop students and unauthorized persons from tampering with the existing school IT infrastructure.

- Strict security must be implemented on the AWS cloud school IT infrastructure, however, will be up to date and more secure than the existing school security.
- School management, staff and IT administrators must understand their responsibilities for security in the cloud.
- Identify laws, regulations and standards that apply to the school such as the Data Protection Act 2018, GDPR, Computer Misuse Act 1990, Online Safety Act 2023.
- Perform a risk assessment to assess risks affecting the school and its IT system and develop a risk management plan.
- Define different security and user roles to prevent unauthorised access to restricted data and prevent unauthorised access and tampering with the school's existing and cloud IT systems.
- Develop security policies, processes, procedures and controls in line with the school's compliance requirements.
- Document controls into a control framework and establish security and privacy controls that meet these requirements.
- Review audit reports and compliance certifications that AWS has in place to understand what security measures they have in place.
- Review security policies, procedures, controls and records as required.
- Use Identity and Access Management (IAM) to define user roles to prevent unauthorized access to restricted data, files and applications, prevent unauthorised access, modification and tampering with administrative software on the AWS cloud school IT system and with AWS components and settings. Use IAM to control which firewall mode each user has such as blocking inappropriate online content.
- Use centralised identity provider to leverage user groups, using strong sign in mechanisms, multifactor authentication, fine grained access.
- Use principle of least privilege and set permissions to prevent unauthorized access to resources.
- Deploy monitoring to analyse data and system events and network traffic to detect threats.
- Regularly scan for vulnerabilities to protect against new threats.
- Use vulnerability scanning software to scan for vulnerabilities.
- Prioritise remediation such as patches and updates to fix vulnerabilities.
- Leverage red teaming and penetration testing to test the school's AWS IT infrastructure for vulnerabilities and exploits.

- Use security groups, firewalls, network access control lists to prevent access to online content that is inappropriate, malicious, illegal, harmful, contains malware, spam or scams or is blocked in accordance with school rules.
- Apply zero trust to systems and data.
- Use virtual private clouds to connect to private cloud components.
- Inspect network traffic.
- Use hardened operating systems and physically secure hybrid cloud infrastructure, on premises infrastructure and edge.
- Prioritise data protection and unauthorized access.
- Encrypt data and files when stored, processed and in transit on network. Require authentication and user roles to access sensitive data.
- Use machine learning to discover, classify and protect sensitive data.
- Define data protection controls and policies.
- Find and fix vulnerabilities in applications during coding phase to save time and money.
- Scan and patch vulnerabilities to protect from new threats.
- Automate security tasks across the school's IT infrastructure cloud.
- Use static code analysis to find common security issues.
- Train IT administrators on how to deal with security incidents.
- Simulate security incidents for incident response training.
- Review security incidents to learn from mistakes and prevent future reoccurrences.

Operations

- Develop telemetry to understand the internal state of the school's cloud IT system for diagnostics and troubleshooting.
- Use canaries (scheduled scripts) to monitor endpoints and APIs.
- Gain insights into resources, servers, applications, databases and networks using metrics and logs.
- Centralise data on a single dashboard to give a unified view of the school's IT system's performance.
- Improve incident response and diagnostics by filtering out noise from operational data.
- Use Machine Learning such as anomaly detection, event correlation and casualty determination to detect problems, threats and incidents.
- Use cloud services for incident management.
- Automate responses to incidents to reduce human error.
- Identify incident patterns to determine problems and corrective measures.
- Track and implement changes using deployment management systems.

- Test changes and analyse results at all department phases to reduce deployment failures.
- Automate rollback in the event of a deployment failure.
- Use quotas to stop a user from using excessive resources.
- Identify key stakeholders to agree on scope, metrics, goals and objectives.
- Evaluate new technologies to improve school cloud IT infrastructure.
- Analyse demand over time to ensure capacity.
- Use tagging schema to overlay school's attributes to its cloud usage.
- Specify mandatory tags and enforce compliance through policy.
- Use Infrastructure as Code (IaC) and configuration tools to provision resources and manage lifecycles.
- Maintain configuration baselines through version control.
- Use patch management to ensure software is up to date and vulnerabilities are fixed.
- Apply updates during scheduled maintenance window (when school is closed) and critical security updates as soon as possible.
- Back up data, documentation, files and applications to a pre-determined schedule for redundancy and disaster proofing.
- Develop a disaster recovery plan for the school's IT systems.
- Identify the level of risk, severity, impact and threat and cost of different disaster scenarios to develop recovery plan.
- Use a single management console to manage the school's cloud-based applications and IT infrastructure.
- Consolidate all operation and management systems into a single console.

Appendix E: Cloud Recommendations

Recommendations for the school's cloud based It system are as follows:

- Use Amazon Web Services (AWS) for the reasons stated above.
- Use private subnets for the school's main IT system, online portals and website development tools for data protection and to prevent unauthorized public access.
- Use a public subnet for the school's website as this is to be viewed by the public.
- Use Region-UK-London to ensure that the data is stored on a UK AWS server to comply with UK data protection, privacy, cybersecurity, online safety, computer misuse and other relevant UK laws due to the sensitive nature of the data held on school IT systems.
- Use an external load balancer to redirect internet traffic to the school website and the internal IT system depending on user role and authentication.

- Use an internal load balancer to redirect school intranet traffic to the IT system's load balancer and the school website.
- Use a load balancer for the school IT system to redirect intrant traffic to the different school IT systems and services.
- Use the AWS firewall to prevent unauthorized access to the school IT infrastructure and systems and data, block inappropriate, offensive and illegal internet content, block malware, hackers, spam and scams and other sites students are not allowed to access in accordance with school rules.
- Use Identity and Access Management (IAM) to define user roles to restrict access to services, software and data depending on the user's role and adopt a zero-trust approach. This will also protect data and prevent unauthorised access to restricted files and applications and prevent unauthorised changes to the IT system and tampering,
- Use a microservice architecture with multiple containers deployed using AWS Elastic Containers Service (ECS) for different school IT system components providing different services to improve maintainability, scalability, elasticity, cross-platform compatibility and reliability.
- Use AWS Elastic Cloud Compute (EC2), Cloud9 IDE and Docker for school software development.
- Use an internal school IT system portal with different microservice containers running different versions of the portal, accessible depending on user role.
- Use AWS CodeCommit Git repository for version control and backups for developing the school's IT system software.
- Use AWS Elastic Block Storage (EBS) to store the school files, data and IT system applications due to the high frequency these files, applications and data will be accessed within the school therefore high-performance block storage is needed instead of S3 buckets.
- Use AWS Simple Storage Service (S3) Buckets to store the files for the school's website and online portal as it is more cost effective than S3 and these files are changed less frequently although the performance on S3 buckets is lower than on AWS EBS.
- Use AWS S3 Glaciers as redundancy to back up all EBS and S3 Bucket storage and the school database(s) for disaster proofing and risk management in the event of data loss, cloud software failure, cyberattack or unauthorised access resulting in the loss of data from them. In the event of a disaster resulting in data loss, restore the data from S3 Glacier backups.
- Use an AWS Relational Database Service (RDS) to host the school's database(s) as an SQL relational database. The various IT system containers that access the database will provide a graphical user interface that allows school staff to easily

interact with the database(s) and automate various IT and school administration and database management tasks.

- The IT systems that I recommend the school migrates to the cloud include the containers in the diagram:
 - School Register and Attendance.
 - Student Records Management System
 - Human Resources Management System
 - Educational software containers
 - IT administration software containers
 - School Administration software containers
 - Marking, Assessment and Grading software
 - Teacher and Class Timetabling software
 - Student Timetabling software
 - Online Teaching System
 - File Management System
 - Communication/Collaboration System
 - Staff Payroll System
 - School Accounting and Finance System
 - Task and Project Management System
 - Assignment, Coursework and Exam Submission System
 - Classwork Submission System
 - Homework Submission System
 - Class Presentation Software containers
 - School Trip Planner Software
 - Student Management System
 - Assistive Technology, Software and Special Needs Software containers.
- Lambda Function for assessing and grading assignments.
- AWS Management and Governance tools to manage the school's cloud IT system:
 - AWS CloudFormation – assist with provisioning, configuring and managing resources.
 - AWS CloudWatch – Monitoring and logging the school's cloud IT infrastructure for diagnostics, troubleshooting, detecting abuse and misuse, cyberbullying on communications and collaboration systems and detecting cybersecurity threats.
 - Config – configure the school's cloud IT infrastructure.
 - Management Console – Manage the school's IT infrastructure.
 - Systems Manager – Incident Manager – Respond to incidents affecting the school's cloud IT infrastructure.
 - Patch Manager – update school IT software hosted on AWS.

- A fast and reliable full-fibre broadband connection and good quality internal networking equipment and infrastructure (routers, switches, hubs, Wireless Access Points, ethernet and fibre optic cables) is strongly recommended for the school due to the vast amount of data constantly travelling between the school's on-site IT infrastructure and computers and mobile devices accessing the cloud and the remote AWS cloud servers hosting the school's cloud IT infrastructure.

Appendix F: Full Cloud Readiness Assessment Report

Full Cloud Readiness Assessment is available here: <https://cloud-computing-diagrams.onrender.com/static/CRA-Report.pdf>

Screenshots of Cloud Readiness Assessment are below (next page).



AWS Cloud Readiness Assessment

Alexander Robertson

s275931@uos.ac.uk

2024-07-03

Disclaimer: Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided ~~as is~~ without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers. © 2024 Amazon Web Services, Inc. or its affiliates. All rights reserved.



About this Report

Thank you for taking the AWS Cloud Readiness Assessment. This tool was produced by AWS.

Services teams using proven frameworks and principles that have helped thousands of customers successfully plan their AWS cloud migrations.

This report helps you understand your cloud readiness scores for each AWS Cloud Adoption Framework (CAF) perspective. It offers additional resources you can use to improve your organization's readiness. A summary of your cloud adoption readiness scores is shown in a heatmap and radar chart, so you can share your organization's results with stakeholders.



Summary of Your Cloud Readiness Scores

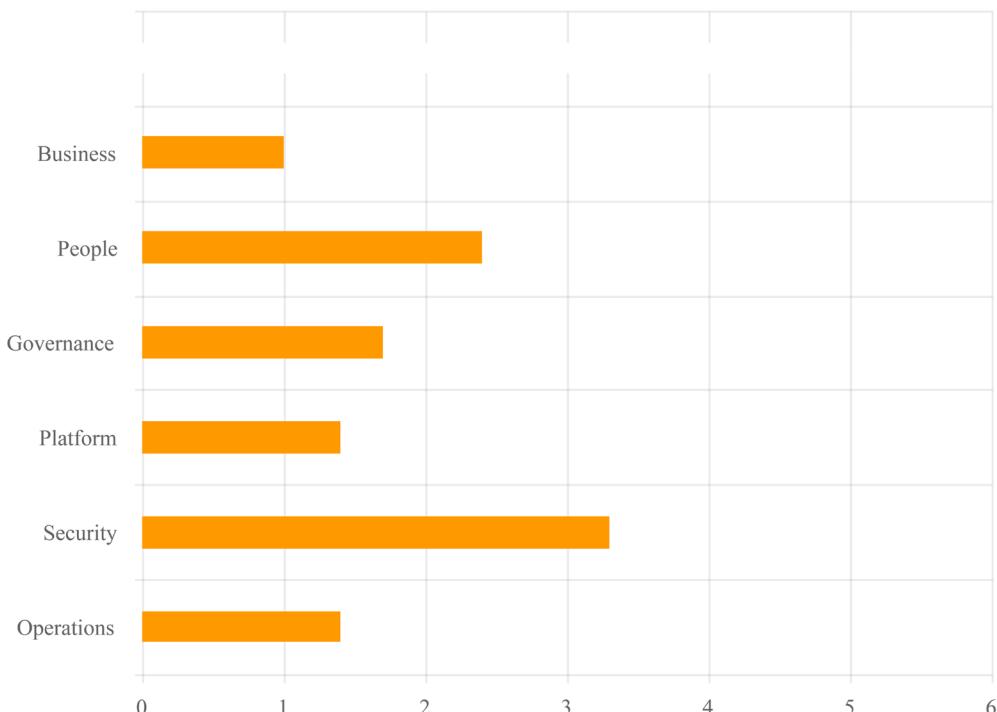
The chart below shows your organization's cloud readiness scores across the six AWS Cloud Adoption Framework (CAF) perspectives, based on the answers you provided for survey questions. [Learn more about CAF.](#)

Green: Questions and Sections that are green indicate a high level of cloud readiness.

Yellow: Questions and Sections that are yellow indicate that additional prep-work is recommended.

Additional resources to help address areas for improvement are provided in this report.

Score Chart

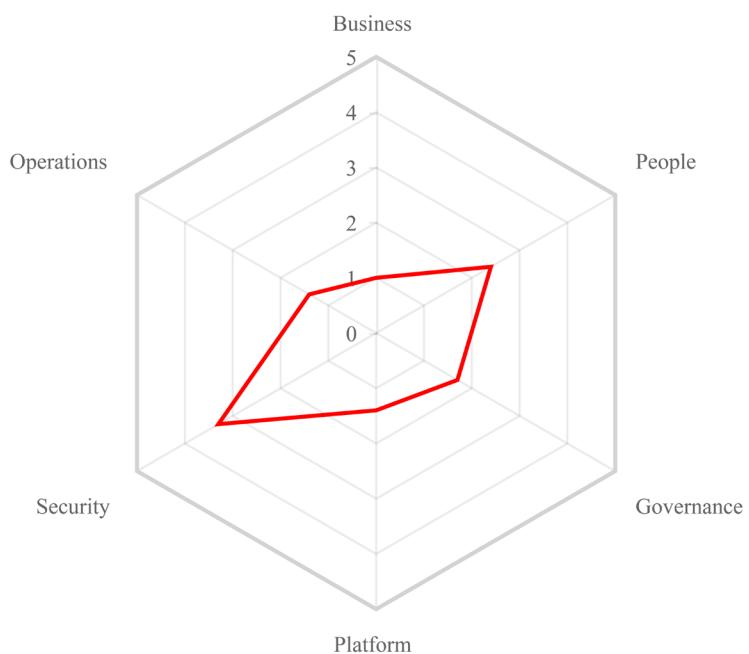




Cloud Readiness Radar Chart

In this section, you will find your assessment scores shown in a radar chart, across the six AWS CAF perspectives. [Learn more about CAF](#).

Visualize your cloud-readiness strengths and weaknesses with the radar chart below, so you can prioritize remediation activities.





Cloud Readiness Heatmap

In this section, you will find your assessment scores shown in a heatmap across the six CAF perspectives. [Learn more about CAF.](#)

Green:Questions and Sections that are green indicate a high level of cloud readiness.

Yellow:Questions and Sections that are yellow indicate that additional prep-work is recommended. Additional resources to help address areas for improvement are provided in this report.

Business

Strategy management
Portfolio management
Innovation management
Product management
Strategic partnership
Data monetization
Business insights
Data science

People

Culture evolution
Transformational leadership
Cloud fluency
Workforce transformation
Change acceleration
Organization design
Organizational alignment

Governance

Program and project management
Benefits management
Risk management
Cloud financial management
Application portfolio management
Data governance
Data curation

Platform

Platform architecture
Data architecture
Platform engineering
Data engineering
Provisioning and orchestration
Modern application development
Continuous integration and continuous delivery

Security

Security governance
Security assurance
Identity and access management
Threat detection
Vulnerability management
Infrastructure protection
Data protection
Application security
Incident response

Operations

Observability
Event management
Incident and problem management
Change and release management
Performance and capacity management
Configuration management
Patch management
Availability and continuity management
Application management



AWS Cloud Readiness Assessment Summary Report

In this section, you will see your responses across the six AWS CAF perspectives. [Learn more about CAF.](#)

Questions and Sections that are green indicate a high level of cloud readiness.

Questions and Sections that are yellow indicate that additional prep-work is recommended. Additional resources to help address areas for improvement are provided in this report.

Business Section

Strategy management

Question: Are you using cloud to enable and shape your long-term business goals?

Response: 1 - No / I don't know.

Rating: 1

Portfolio management

Question: Are you prioritizing your cloud initiatives in line with your strategic intent, operational efficiency, and your capacity to deliver?

Response: 1 - No / I don't know.

Rating: 1

Innovation management

Question: Are you leveraging cloud to develop new, and improve existing, processes, products, and experiences?

Response: 1 - No / I don't know.

Rating: 1



Product management

Question: Do you organize your cross-functional teams around cloud-enabled digital products?

Response: 1 - No / I don't know.

Rating: 1

Strategic partnership

Question: Are you leveraging your cloud provider to build or grow your business?

Response: 1 - No / I don't know.

Rating: 1

Data monetization

Question: Have you identified opportunities for leveraging data to improve operations, customer and employee experience, decision-making, or to enable new business models?

Response: 1 - No / I don't know.

Rating: 1

Business insights

Question: Are you able to gain real-time insights and answer questions about your business?

Response: 1 - No / I don't know.

Rating: 1

Data science

Question: Do you leverage experimentation, advanced analytics, and machine learning to solve complex



business problems?

Response: 1 - No / I don't know.

Rating: 1

Recommended Actions:

Strategy management

Identify opportunities for [retiring technical debt](#) and leverage cloud to optimize your [technology](#) and [business operations](#).

Explore new cloud-enabled [value propositions](#) and revenue models.

Consider how new or improved cloud-enabled products and services can help you reach [new customers](#) or enter new market segments.

Prioritize your strategic objectives and evolve your strategy over time in response to technological developments and changes in your business environment.

Portfolio management

Leverage automated discovery [tools](#) and the seven common migration strategies for moving applications to the cloud (known as the [7 Rs](#)) to rationalize your existing application portfolio and build a data-driven [business case](#).

Balance your cloud portfolio by considering short-term and long-term outcomes as well as low-risk (proven) and higher-risk (experimental) opportunities.

Include [migration](#), [modernization](#), and [innovation](#) initiatives, and consider financial and non-financial benefits.

Optimize the business value of your portfolio in line with your resource, financial, and schedule constraints.

To reduce your [time-to-value](#), consider increasing the frequency of your planning cycles or adopting a continuous planning strategy.

Innovation management

Develop an innovation strategy that includes a mix of incremental innovation initiatives focused on optimizing your existing products, processes, and experiences, as well as disruptive innovation initiatives focused on enabling new business models.

Create mechanisms for soliciting and selecting ideas in line with your strategic priorities, and develop an end-to-end process for scaling successful innovation pilots.



Product management

Develop a balanced product portfolio that supports your business strategy.

Establish small, enduring, and empowered cross-functional teams that champion the needs of internal and external customers.

Identify product owners, understand customer journeys, define and create product roadmaps, and manage end-to-end product lifecycles and associated value streams.

Leverage your cloud platform and agile methods to rapidly iterate and evolve.

Reduce dependencies between product teams and effectively integrate them into your broader operating model via well-defined interfaces.

Strategic partnership

If you offer cloud-hosted software solutions, cloud-integrated products, or cloud-related professional, consulting, or managed services, **strategically partnering** with your cloud provider can help you build your **cloud expertise**, **promote your solutions** to customers, and drive successful **customer engagements**.

As you progress along your partnership journey, leverage **promotional credits, funding benefits**, and co-selling opportunities to help you **build or grow your business**.

Leverage your cloud provider's **marketplace** channel to expand reach, and technical resources to help you mature your **cloud-based products and services**.

Publish joint case studies to highlight success in solving specific business challenges.

Data monetization

To obtain measurable business benefits, develop a comprehensive and long-term **data monetization strategy** that is aligned with your strategic intent.

Focus on transactional value that helps you understand and complete business transactions, informational value that helps you describe past performance and infer conclusions, and analytical value that helps you automate activities, guide decisions, and predict outcomes.

Monetize data internally within your organization before considering opportunities for external monetization (for example, selling data via a marketplace).

Business insights

Establish cross-functional analytics teams with a good understanding of the business context.

Focus on technical (such as statistics) and non-technical (such as visualization and communication) skills.

Align your analytics efforts with business goals and key performance indicators (KPIs).



Leverage a [Data Catalog](#) to locate relevant data products, and visualization tools and techniques to discover trends, patterns, and relationships in the data.

Focus on the [big picture](#) first and drill down into the details as required.

Data science

Once you've identified opportunities for business process transformation, ensure that your [Data Catalog](#) contains the data products required to support the building, training, and testing of your machine learning models.

Leverage [continuous integration and continuous delivery](#) (CI/CD) practices to improve operational resilience and reproducibility of your machine learning workflows.

Understand how your models make predictions and identify any potential biases.

Deploy suitable models to production and monitor their performance.

To mitigate risk, delegate low confidence predictions for human review.



People Section

Culture evolution

Question: Do you have a plan to evolve your organizational culture in line with your digital transformation aspirations?

Response: 2 - Starting to think about it.

Rating: 2

Transformational leadership

Question: Are your leaders driving transformational change while enabling outcome-focused, cross-functional decision making?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Cloud fluency

Question: Are you building digital acumen to confidently and effectively leverage cloud to accelerate your business outcomes?

Response: 1 - No / I don't know.

Rating: 1

Workforce transformation

Question: Are you attracting, developing, and retaining a digitally fluent high-performing and adaptable workforce?

Response: 3 - Experimenting with pilot initiatives.



Rating: 3

Change acceleration

Question: Are you accelerating adoption to the new ways of working by applying a programmatic change acceleration framework?

Response: 2 - Starting to think about it.

Rating: 2

Organization design

Question: Are you evolving your organizational structure as you progress through your transformation journey?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Organizational alignment

Question: Have you established ongoing partnership between business and technology teams?

Response: 2 - Starting to think about it.

Rating: 2

Recommended Actions:

Culture evolution

To succeed in digital transformation, you'll need to leverage your heritage and core values, while you incorporate new behaviors and mindsets that attract, retain, and empower a workforce that's invested in continuously improving and innovating on behalf of your customers.

Maintain a long-term focus, obsess over customers, and boldly innovate to meet their needs.



Institute an organization-wide [approach](#) to recognizing behaviors and goals for all roles that help shape your desired culture.

Consider [rapid experimentation](#), agile methodologies, and cross-functional teams to drive ownership and autonomy, enable rapid decision making, and minimize the need for excessive approvals or bureaucracy.

See [AWS Cloud Adoption Framework](#) for additional guidance.

Transformational leadership

Gain active and visible executive sponsorship from both technology and business functions, who will make critical decisions on strategy, vision, scope, and resources, and take actions in communication, coalition building, and holding teams accountable for results.

At both the executive and program levels, ensure that your business and technology leaders co-develop, co-lead, and co-deliver culture change strategies.

Confirm that each [layer of management](#) delivers clear and consistent communications to align the organization on cloud value, priorities, and new behaviors.

Consider evolving your cloud leadership function through a transformation office and/or a [Cloud Center of Excellence](#) (CCoE) to evangelize and drive your transformation efforts with codified patterns for consistency and scalability.

Incrementally evolve this function to meet your current needs as you progress through your transformation journey.

Cloud fluency

Address your overall training strategy as it relates to timing, tooling, and technology training, and then [assess](#) your existing cloud skills to develop a [targeted training strategy](#).

Implement a [skills guild](#) to help you generate excitement and build momentum for your transformation journey.

Champion [data literacy](#) to advance talent skills and knowledge in data analytics.

Combine virtual, classroom, experiential and just-in-time [training](#), leverage [immersion days](#), and validate skills with formal [certifications](#).

Implement mentoring, coaching, shadowing, and job rotation programs.

Set up communities of practice that own specific domains of interest.

Reward individuals for sharing knowledge, and formalize processes for knowledge elicitation, peer review, and ongoing curation.



Workforce transformation

To succeed in your cloud transformation, take a proactive approach to [talent enablement](#) planning beyond traditional HR to include C-suite leadership, and modernize your approaches to leadership, learning, rewards, inclusion, performance management, career mobility, and hiring.

Identify gaps in roles and skills across your entire organization and develop a workforce strategy that will improve your organizational cloud capability.

Leverage talent with digital skills, and those that are eager to learn, and make an example of them.

Strategically consider the use of [partners](#) and [managed service providers](#) to temporarily or permanently augment your workforce.

To attract new talent, build a strong employer brand by publicly promoting your digital vision and organizational culture, and use it in your recruiting strategy, social networking channels, and external marketing.

Change acceleration

Align and mobilize cross-functional cloud leadership.

Define what success looks like early in the journey.

Envision the future by assessing your organization's readiness for cloud through impact assessments.

Identify key stakeholders, cross-organizational dependencies, key risks, and barriers to transformation.

Develop a [change acceleration strategy](#) and roadmap that addresses risks and leverages strengths, comprised of leadership action plans, talent engagement, communications, training, and risk mitigation strategies.

Engage the organization and enable it with new capabilities to increase acceptance to the new ways of working, learn new skills, and accelerate adoption.

Track clearly defined metrics and celebrate early wins.

Establish a change coalition to leverage existing cultural levers that can help you generate momentum.

Make changes stick with continuous feedback mechanisms, and rewards and recognition programs.

Organization design

As you leverage cloud to digitally transform, ensure your organization design supports your core strategies for the business, its people, and operating environment.

Establish a case for change, and assess if your organization design reflects the desired behaviors, roles, and culture that you have determined are key elements to your business success.



Determine if the way your organization is structured and run, in terms of team formations, shift patterns, lines of reporting, decision-making procedures, and communication channels, still supports your desired business outcomes.

Design the new model, and implement it by applying your change acceleration framework.

Consider establishing a [centralized team](#) that is built to evolve over time, and which will initially facilitate and enable the transition to a [cloud operating model](#) that may be tailored to your vision.

Consider trade-offs between centralized, decentralized, and distributed structures, and align your organization design to support the strategic value of your cloud workloads.

Clarify the relationships between internal and external teams (such as [managed service providers](#)).

Organizational alignment

Set measurable targets, joint goals, and mechanisms for cloud adoption, and create expectations for skill development at the role level to generate sustainable change ownership.

Take a top-down approach to developing shared values, processes, systems, working styles, and skills to collectively drive business outcomes and break down functional silos.

Tie innovation efforts to customer experience.

Recognize and reward those who continuously adopt and innovate.



Governance Section

Program and project management

Question: Are you delivering interdependent cloud initiatives in a flexible and coordinated manner?

Response: 1 - No / I don't know.

Rating: 1

Benefits management

Question: Are you ensuring that the business benefits associated with your cloud investments are realized and sustained?

Response: 1 - No / I don't know.

Rating: 1

Risk management

Question: Are you leveraging cloud to lower your risk profile?

Response: 1 - No / I don't know.

Rating: 1

Cloud financial management

Question: Do you plan, measure, and optimize your cloud spend?

Response: 1 - No / I don't know.

Rating: 1

Application portfolio management



Question: Are you managing and optimizing your application portfolio in support of your business strategy?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Data governance

Question: Are you able to exercise authority and control over your data to meet stakeholder expectations?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Data curation

Question: Are you leveraging metadata to organize an inventory of data products in a Data Catalog?

Response: 1 - No / I don't know.

Rating: 1

Recommended Actions:

Program and project management

Manage interdependencies by aligning multiple initiatives for optimized or integrated costs, schedule, effort, and benefits.

Regularly validate your roadmap with your business sponsors and escalate any issues to the senior leadership in a timely fashion to drive accountability and transparency.

Adopt an agile approach to minimize the need to make far-reaching predictions, instead, allowing you to learn from experience and adapt as you progress through your transformation journey.

To help you respond to change, produce well-prioritized backlogs and structure your work in the form of epics and stories.

Benefits management



Identify metrics, [quantify desired benefits](#), and communicate to the relevant stakeholders.

Align the timing and life-span of benefits with your strategic goals.

Incorporate benefits delivery into a benefits realization roadmap.

Regularly measure realized benefits, evaluate progress against the benefits realization roadmap, and adjust the expected benefits as required.

Risk management

Identify and quantify operational [risks](#) relating to infrastructure availability, reliability, performance, and security, and business risks relating to reputation, business continuity, and your ability to quickly respond to changing market conditions.

Understand how cloud can help you reduce your risk profile and continue to iteratively identify and manage risk as part of your agile cadence.

Consider leveraging cloud to reduce risks relating to infrastructure operation and failure.

Depending on the needs of your users, mitigate procurement schedule risks by leveraging cloud to instantly provision and deprovision resources.

Cloud financial management

Clarify [financial roles and responsibilities](#) as they pertain to cloud, and ensure that key stakeholders across your finance, business and technology organizations have a [shared understanding](#) of cloud costs.

Evolve to a more [dynamic forecasting](#) and [budgeting](#) process, and identify [cost variances](#) and [anomalies](#) faster.

Align your [account structure](#) and [tagging strategy](#) with how your organization and products map to the cloud.

Structure your accounts and [cost allocations tags](#) to map your cloud resources to specific teams, projects, and business initiatives, and gain a [granular](#) view of your consumption patterns.

Define [cost categories](#) to organize your cost and usage information using custom rules to simplify showback or chargeback.

Use [consolidated billing](#) to help simplify cloud billing and realize [volume discounts](#).

Build [guardrails](#) to govern your cloud usage in a scalable manner and with minimal impact to agility.

Leverage [demand-based](#) and [time-based](#) dynamic provisioning to pay only for the resources you need.

Reduce cloud costs by [identifying and eliminating](#) spend associated with [idle or underutilized](#) cloud resources.

Centralize the [management](#) of on-premises and cloud software licenses to reduce license-related cost overages, reduce non-compliance, and avoid misreporting.



Application portfolio management

An accurate and complete application inventory will help you identify opportunities for rationalization, [migration](#), and modernization.

An effective application portfolio management capability will help you minimize application sprawl, facilitate application lifecycle planning, and ensure ongoing alignment with your cloud transformation strategy.

Start with your most critical applications, define them in terms of the overarching business capabilities, and map them to the underpinning software products and associated resources.

Build a complete picture of each application by sourcing data from related enterprise systems, such as enterprise architecture, IT service management (ITSM), and project and portfolio management.

Identify key technology and business stakeholders (including application owners) and request them to periodically enrich and validate application metadata.

Assess the health of your application portfolio on a regular basis with a view to maximizing the value that your organization derives from its application investments.

Data governance

Define and assign key roles, including data owners, stewards, and custodians.

Consider adopting a federated ([data mesh](#)) approach to governance.

Specify standards, including data dictionaries, taxonomies, and business glossaries.

Identify what datasets need to be referenced and model the relationships between reference data entities.

Develop [data lifecycle](#) policies, and implement continuous compliance monitoring.

Prioritize your [data quality](#) efforts in line with your strategic and operational data needs.

Establish data quality standards: identify key quality attributes, business rules, metrics, and targets.

Monitor data quality at every step of the data value chain.

Identify root causes of data quality problems and improve relevant processes at the source.

Implement data quality dashboards for critical data products.

Data curation

Identify lead curators with responsibility for moderating the Data Catalog.

In line with your data monetization strategy, catalog key data products, including structured and unstructured data.

Identify and capture relevant technical and business metadata, including lineage.



Leverage standard ontologies, business glossaries, and automation (including machine learning) to tag, index, and auto-classify data.

Augment with manual tagging as necessary and appropriately handle any personally identifiable information (PII).

Consider crowdsourcing data enrichment through social curation; consider empowering data consumers to rate, review, and annotate data products.



Platform Section

Platform architecture

Question: Are you establishing and maintaining guidelines, principles, patterns, and guardrails for your cloud environment?

Response: 2 - Starting to think about it.

Rating: 2

Data architecture

Question: Are you designing and evolving a fit-for-purpose data and analytics architecture?

Response: 2 - Starting to think about it.

Rating: 2

Platform engineering

Question: Have you built a compliant multi-account cloud environment with enhanced security features, and packaged, reusable cloud products?

Response: 2 - Starting to think about it.

Rating: 2

Data engineering

Question: Do you automate and orchestrate data flows across your organization?

Response: 1 - No / I don't know.

Rating: 1



Provisioning and orchestration

Question: Are you creating, managing, and distributing catalogs of approved cloud products to end users?

Response: 1 - No / I don't know.

Rating: 1

Modern application development

Question: Do you build well-architected cloud-native applications?

Response: 1 - No / I don't know.

Rating: 1

Continuous integration and continuous delivery

Question: Are you evolving and improving applications and services at a faster pace than organizations using traditional software development and infrastructure management processes?

Response: 1 - No / I don't know.

Rating: 1

Recommended Actions:

Platform architecture

A [well-architected cloud environment](#) will help you accelerate implementation, reduce risk, and drive cloud adoption.

Create consensus within your organization for enterprise standards that will drive cloud adoption.

Define best practice [blueprints](#) and [guardrails](#) to facilitate [authentication](#), [security](#), [networking](#), and [logging and monitoring](#).

Consider what workloads you may need to retain [on-premises](#) due to latency, data processing, or data residency requirements.



Evaluate such hybrid cloud [use cases](#) as cloud bursting, backup and disaster recovery to the cloud, distributed data processing, and edge computing.

Data architecture

A [well-designed](#) data and analytics [architecture](#) can help you reduce complexity, cost, and technical debt while enabling you to gain actionable insights from exponentially growing data volumes.

Adopt a layered and modular architecture that will allow you to use the right tool for the right job as well as iteratively and incrementally evolve your architecture to meet emerging requirements and use cases.

Based on your requirements, select key technologies for each of your [architectural layers](#), including ingestion, storage, catalog, processing, and consumption.

To simplify ongoing management, consider adopting [serverless](#) technologies.

Focus on supporting real-time data processing, and consider adopting a [modern data architecture](#) to facilitate data movements between data lakes and purpose-built data stores.

Platform engineering

Deploy your best practice blueprints, and detective and preventative [guardrails](#).

[Integrate](#) your cloud environment with your existing ecosystem to enable desired hybrid cloud use cases.

Automate the account provisioning workflow and leverage [multiple accounts](#) to support your security and governance goals.

Set up connectivity between your on-premises and cloud environments as well as between different cloud accounts.

Implement [federation](#) between your existing identity provider (IdP) and your cloud environment so that users can authenticate using their existing login credentials.

Centralize logging, establish cross-account security audits, create inbound and outbound Domain Name System (DNS) resolvers, and get dashboard visibility into your accounts and guardrails.

Evaluate and certify cloud services for consumption in alignment with corporate standards and configuration management.

Package and continuously improve enterprise standards as self-service deployable products and consumable services.

Leverage [infrastructure as code](#) (IaC) to define configurations in a declarative way.

Data engineering

Automated data and analytics platforms and pipelines may help you improve productivity and accelerate time



to market.

Form cross-functional data engineering teams comprising infrastructure and operations, software engineering, and data management.

Leverage metadata to automate [pipelines](#) that consume raw and produce optimized data.

Implement relevant architectural guardrails and security controls, as well as monitoring, logging, and alerting to help with pipeline failures.

Identify common data integration patterns and build reusable [blueprints](#) that abstract away the complexity of pipeline development.

Share blueprints with business analysts and data scientists and enable them to operate using self-service methods.

Provisioning and orchestration

Maintaining consistent infrastructure provisioning in a scalable and repeatable manner becomes more complex as your organization grows.

Streamlined [provisioning and orchestration](#) help you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved cloud products.

Design and implement a centrally-managed, [self-service portal](#) for publishing, [distributing](#), browsing, and consuming approved cloud products.

Make your cloud products accessible via APIs as well as via personalized portals.

Integrate with your IT service management (ITSM) [tools](#) and automate any updates to your configuration management database (CMDB).

Modern application development

[Modern application](#) development practices can help you realize the speed and agility that go with innovation.

Using [containers](#) and [serverless](#) technologies can help you optimize your resource utilization and automatically scale from zero to peak demands.

Consider decoupling your applications by building them as independent [microservices](#) leveraging [event-driven](#) architectures.

Implement security in all layers and at each stage of the application development lifecycle.

Automate the process of scaling out and scaling in or use serverless technologies.

[Modernize](#) your existing applications to reduce costs, gain efficiencies, and make the most of your existing investments.



Consider [replatforming](#) (moving your own containers, databases, or message brokers to managed cloud services) and [refactoring](#) (rewriting your legacy applications to a cloud native architecture).

Ensure that your architecture takes into account [service quotas](#) and physical resources so that they do not negatively impact your workload performance or reliability.

Continuous integration and continuous delivery

Adopting [DevOps](#) practices with [continuous integration](#), testing, and [deployment](#) will help you to become more agile so that you can innovate faster, adapt to changing markets better, and grow more efficient at driving business results.

Implement continuous integration and continuous delivery (CI/CD) [pipelines](#).

Start with a minimum viable pipeline for continuous integration and then transition to a [continuous delivery](#) pipeline with more components and stages.

Encourage [developers](#) to create unit tests as early as possible and to run them before pushing the code to the central repository.

Include staging and production steps in your continuous delivery pipeline and consider manual approvals for production deployments.

Consider multiple [deployment strategies](#), including in-place, rolling, immutable, and blue/green deployments.



Security Section

Security governance

Question: Are you developing, maintaining, and effectively communicating security roles, responsibilities, accountabilities, policies, processes, and procedures?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Security assurance

Question: Are you continuously monitoring, evaluating, managing, and improving the effectiveness of your security and privacy programs?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Identity and access management

Question: Are you effectively managing identities and permissions at scale?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Threat detection

Question: Do you understand and identify potential security misconfigurations, threats, or unexpected behaviors?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4



Vulnerability management

Question: Are you continuously identifying, classifying, remediating, and mitigating security vulnerabilities?

Response: 2 - Starting to think about it.

Rating: 2

Infrastructure protection

Question: Are you validating that systems and services within your workload are protected against unintended and unauthorized access and potential vulnerabilities?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Data protection

Question: Do you maintain visibility and control over data, and how it is accessed and used in your organization?

Response: 4 - Yes, but inconsistently implemented across the organization.

Rating: 4

Application security

Question: Do you detect and address security vulnerabilities during the software development process?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Incident response



Question: Are you reducing potential harm by effectively responding to security incidents?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Recommended Actions:

Security governance

Understand your responsibility for [security in the cloud](#).

Inventory, categorize, and prioritize relevant stakeholders, assets, and information exchanges.

Identify laws, rules, regulations, and [standards/frameworks](#) that apply to your industry and/or organization.

Perform an annual risk assessment on your organization; risk assessments can assist in determining the likelihood and impact of identified risks and/or vulnerabilities affecting your organization.

Allocate sufficient resources to identified security roles and responsibilities.

Develop security policies, processes, procedures, and controls in line with your compliance requirements and organizational risk tolerance; continuously update based on evolving risks and requirements.

Security assurance

Document controls into a comprehensive [control framework](#), and establish demonstrable security and [privacy](#) controls that meet those objectives.

Review the [audit reports](#), compliance [certifications, or attestations](#) that your cloud vendor has obtained to help you understand the controls they have in place, how those controls have been validated, and that controls in your extended IT environment are operating effectively.

Continuously [monitor and evaluate](#) your environment to verify the operating effectiveness of your controls, and demonstrate compliance with regulations and industry standards.

Review security policies, processes, procedures, controls, and records, and interview key personnel as required.

Identity and access management

Effective [identity and access management](#) helps validate that the right people and machines have access to the right resources under the right conditions.

The [AWS Well-Architected Framework](#) describes relevant concepts, design principles, and architectural best practices to manage [identities](#). These include: relying on a centralized identity provider; leveraging user groups



and attributes for fine-grained access at scale and temporary credentials; and using strong sign-in mechanisms, such as multi-factor authentication (MFA).

To [control access](#) by human and machine identities to AWS and your workloads, set permissions to specific service actions on specific resources under specific conditions; use the principle of least privilege, set permissions boundaries, and use service control policies so the right entities can access the right resources as your environment and user base grow; grant permissions based on attributes (ABAC) so your policies can scale; and continuously validate that your policies provide the protection that you need.

Threat detection

Agree on tactical, operational, and strategic intelligence goals and overall methodology.

Mine relevant data sources, process and analyze data, and disseminate and operationalize insights.

Deploy [monitoring](#) ubiquitously within the environment to collect essential information and at ad hoc locations to track specific types of transactions.

Correlate monitoring data from [multiple event sources](#), including network traffic, operating systems, applications, databases, and endpoint devices to provide a robust security posture and enhance visibility.

Vulnerability management

Regularly [scan](#) for vulnerabilities to help protect against new threats.

Employ vulnerability [scanners](#) and endpoint agents to associate systems with known vulnerabilities.

Prioritize remediation actions based on the vulnerability risk.

Apply remediation actions and report to relevant stakeholders.

Leverage red teaming and [penetration testing](#) to identify vulnerabilities in your system architecture; seek prior authorization from your cloud provider as required.

Infrastructure protection

Leverage [defense in depth](#) to layer a series of defensive mechanisms aimed at protecting your data and systems.

Create network layers and place workloads with no requirements for internet access in private subnets.

Use [security groups](#), [network access control lists](#), and [network firewalls](#) to control traffic.

Apply [Zero Trust](#) to your systems and data in accordance with their value.

Leverage virtual private cloud (VPC) [endpoints](#) for private connection to cloud resources.

Inspect and filter your traffic at each layer; for example, via a [web application firewall](#) and/or a [network](#)



firewall .

Use hardened operating system images and physically secure any [hybrid](#) cloud infrastructure on-premises and at the [edge](#).

Data protection

[Protecting](#) your data from unintended and unauthorized access, and potential vulnerabilities, is one of the key objectives of your security program.

In order to help you determine appropriate protection and retention controls, [classify](#) your data based on criticality and sensitivity (for example, personally identifiable information).

Define data protection controls and [lifecycle](#) management policies.

Encrypt all data at rest and in transit, and store sensitive data in separate accounts.

Leverage machine learning to automatically [discover](#), classify, and protect sensitive data.

Application security

You can save time, effort, and cost when you find and remediate security flaws during the coding phase of an application, and have confidence in your security posture as you launch into production.

Scan and patch for vulnerabilities in your code and dependencies to help protect against new threats.

Minimize the need for human intervention by [automating](#) security-related tasks across your development and operations processes and tools.

Use static code analysis [tools](#) to identify common security issues.

Incident response

[Educate](#) your security operations and incident response teams about cloud technologies and how your organization intends to use them.

Develop [runbooks](#) and create a library of incident response mechanisms. Include key stakeholders to better understand the impact of your choices on the broader organization.

[Simulate](#) security events and practice your incident response through table-top exercises and game days.

[Iterate](#) on the outcome of your simulation to improve the scale of your response posture, reduce time to value, and further reduce risk.

Conduct post-incident analyses to learn from security incidents by leveraging a standardized mechanism to identify and resolve [root causes](#).



Operation Section

Observability

Question: Are you gaining actionable insights from your infrastructure and application data?

Response: 1 - No / I don't know.

Rating: 1

Event management

Question: Are you effectively detecting events, assessing their potential impact, and determining appropriate control actions?

Response: 3 - Experimenting with pilot initiatives.

Rating: 3

Incident and problem management

Question: Do you quickly restore service operations and minimize adverse business impact?

Response: 1 - No / I don't know.

Rating: 1

Change and release management

Question: Are you introducing and modifying workloads while minimizing the risk to production environments?

Response: 1 - No / I don't know.

Rating: 1



Performance and capacity management

Question: Are you monitoring workload performance while ensuring that capacity meets current and future demands?

Response: 1 - No / I don't know.

Rating: 1

Configuration management

Question: Are you maintaining an accurate and complete record of all your cloud workloads, their relationships, and configuration changes over time?

Response: 1 - No / I don't know.

Rating: 1

Patch management

Question: Are you systematically distributing and applying software updates?

Response: 2 - Starting to think about it.

Rating: 2

Availability and continuity management

Question: Are you effectively ensuring availability of business-critical information, applications, and services?

Response: 2 - Starting to think about it.

Rating: 2

Application management



Question: Are you investigating and remediating application issues in a single pane of glass?

Response: 1 - No / I don't know.

Rating: 1

Recommended Actions:

Observability

Develop the [telemetry](#) (logs, metrics, and traces) necessary to understand the [internal state](#) and health of your workloads.

Monitor application endpoints, assess the impact to the end users, and generate alerts when measurements exceed thresholds.

Use [synthetic monitoring](#) to create canaries (configurable scripts that run on a schedule) to monitor your endpoints and APIs.

Implement [traces](#) to track requests as they travel through the entire application and identify bottlenecks or performance issues.

Gain [insights](#) into resources, servers, databases, and networks using metrics and logs.

Set up real-time analysis of time series data to understand causes of performance impacts.

Centralize data in a single [dashboard](#), giving you a [unified view](#) of critical information about your workloads and their performance.

Event management

Being able to filter the noise, focus on priority events, predict impending resource exhaustion, automatically generate alerts and incidents, and identify likely causes and remediation actions will help you improve incident detection and response times.

Establish an event store pattern and leverage [machine learning \(AIOps\)](#) to automate event correlation, anomaly detection, and causality determination.

Integrate with [cloud services](#) and third-party tools, including with your incident management system and process.

Automate responses to events to reduce errors caused by manual processes and ensure prompt and consistent responses.



Incident and problem management

Practice incident response [gamedays](#) and incorporate lessons learned in your runbooks.

Identify incident patterns to determine problems and corrective measures.

Leverage [chatbots](#) and collaboration tools to connect your operations teams, tools, and workflows.

Leverage blameless [post-incident analyses](#) to identify contributing factors of incidents and develop corresponding action plans.

Change and release management

Establish [change processes](#) that allow for automated approval [workflows](#) that align with the [agility of the cloud](#).

Use deployment management systems to track and implement changes.

Use [frequent](#), small, and reversible changes to reduce the scope of a change.

Test changes and validate the results at all [lifecycle stages](#) to minimize the risk and impact of failed deployments.

Automate rollback to previous known good state when outcomes are not achieved to minimize recovery time and reduce errors caused by manual processes.

Performance and capacity management

Although the capacity of the cloud is virtually unlimited, [service quotas](#), [capacity reservations](#), and resource constraints restrict the actual capacity of your workloads. Such capacity constraints need to be [understood](#) and effectively [managed](#).

Identify key stakeholders and agree on the objectives, scope, goals, and metrics.

Collect and process performance data and regularly [review](#) and report performance against targets.

Periodically evaluate new technologies to improve performance and recommend changes to the goals and metrics as appropriate.

Monitor the utilization of your workloads, create baselines for future comparison, and identify thresholds to expand capacity as required.

Analyze demand over time to ensure capacity matches seasonal trends and fluctuating operating conditions.

Configuration management

Define and enforce a [tagging schema](#) that overlays your business attributes to your cloud usage, and leverage tags to organize your resources along technical, business, and security dimensions.



Specify mandatory tags and enforce [compliance](#) through policy.

Leverage [infrastructure as code](#) (IaC) and configuration management [tools](#) for resource provisioning and [lifecycle management](#).

Establish configuration [baselines](#) and maintain them through [version control](#).

Patch management

A systematic approach to [patch management](#) will ensure that you benefit from the latest updates while minimizing risks to production environments.

[Apply](#) important updates during your specified [maintenance window](#) and critical security updates as soon as possible.

Notify users in advance with the details of the upcoming updates and allow them to defer patches when other mitigating controls are available.

Update your machine images and test patches before rolling out to production.

To ensure continued availability during patching, consider separate maintenance windows for each Availability Zone (AZ) and environment.

Regularly review patching compliance and alert non-compliant teams to apply required updates.

Availability and continuity management

Back up your data and documentation according to a defined schedule.

Develop a disaster recovery plan as a subset of your business continuity plan.

Identify the threat, risk, impact, and cost of different disaster scenarios for each workload and specify Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) accordingly.

Implement your chosen disaster recover [strategy](#) leveraging multi-AZ or multi-Region architecture.

Consider leveraging [chaos engineering](#) to improve resiliency and performance with controlled experiments.

Review and test your plans regularly and adjust your approach based on lessons learned.

Application management

Aggregating application data into a [single management console](#) will simplify operational oversight and accelerate remediation of application issues by reducing the need to switch context between different management tools.

[Integrate](#) with other operational and management systems, such as application portfolio management and CMDB, [automate](#) the discovery of your application components and resources, and consolidate application data



into a single management console.

Include software components and infrastructure resources, and delineate different environments, such as development, staging, and production.

To remediate operational issues more quickly and consistently, consider automating your [runbooks](#).



How to Use This Report to Advance Your Cloud Readiness

In preparing for an AWS Cloud migration, we recommend that you review the checklist below as your next step:

1. Review the [AWS Migration Readiness Guide](#). This guide walks readers through what it means to be ready to migrate and how to establish a solid foundation to save time and prevent roadblocks. We discuss the impact and importance of driving organizational change, preparing leadership, and establishing foundational readiness for large-scale migrations. We also present our iterative methodology for executing a successful migration.
2. Next, we encourage customers to use our AWS CAF to help address the six perspectives responded to in the Survey. AWS created the [Cloud Adoption Framework \(AWS CAF\) whitepaper](#) to help organizations develop efficient and effective plans for their cloud adoption journey. Each CAF perspective is used to create work streams that uncover gaps in your existing skills and processes.
3. Often customers require specialized skills and experience to help supplement their team. AWS offers professional services to help you realize your desired business outcomes. If you would like to request an executive briefing or consultation please contact your sales representative. If you are new to AWS, you may use this [link](#) to request support.

Further Reading:

For additional information, tools and customer case studies please consult the following resources:

[AWS Migration](#)

[AWS Migration Acceleration Program \(MAP\)](#)

[AWS Migration Hub](#)