



Education Solutions

The Holistic Data Approach to Student Success



Predictive Analytics

Turn data into insight, and insight into action.

[READ MORE](#)



Student Management

Teaching takes more than teaching.

[READ MORE](#)



Observation and Growth

Are you mentoring your teachers, or are you telling them facts? There's a difference.

[READ MORE](#)

March 20, 2019 | ClassMate in AWS





Why AWS, Why now, What to expect?





Microsoft
SQL Server 2017

Benefits

From old

- SQL Server 2000 (Win 2003)
- Citrix/XenCenter 6.2
- Aged host servers and SAN

To new

- SQL Server 2017
- Reliability/Resiliency/ Scalability
- Improved Compliance:
FERPA/NIST 800/NY Education
Law 2-d

AWS Services in Scope by Compliance Program

We include services in the scope of our compliance efforts based on the expected use case, feedback and demand. If a service is not currently listed as in scope of the most recent assessment, it does not mean that you cannot use the service. It is part of the **shared responsibility** for your organization to determine the nature of the data. Based on the nature of what you are building on AWS, you should determine if the service will process or store customer data and how it will or will not impact the compliance of your customer data environment.

We encourage you to discuss your workload objectives and goals with your AWS account team; they will be able to evaluate your proposed use case and architecture, and how our security and compliance processes overlay that architecture. **Need to connect with an AWS business representative?**

This webpage provides a list of AWS Services in Scope of AWS assurance programs. Unless specifically excluded, features of each of the services are considered in scope of the assurance programs, and are reviewed and tested as part of the assessment. Refer to the AWS Documentation for the features of an AWS service

✓ = This service is currently in scope and is reflected in current reports


Joint Authorization Board (JAB) Review = This service is currently undergoing a JAB Review

Third Party Assessment Organization (3PAO) = This service is currently undergoing an assessment by our third party assessor

SOC	PCI	ISO	FedRAMP	DoD CC SRG	HIPAA BAA	IRAP	MTCS	C5	K-ISMS	ENS High
SERVICES / PROGRAMS				FedRAMP Moderate (East/West)			FedRAMP High (GovCloud)			
Amazon API Gateway			✓							JAB Review
Amazon Athena						3PAO Assessment				3PAO Assessment

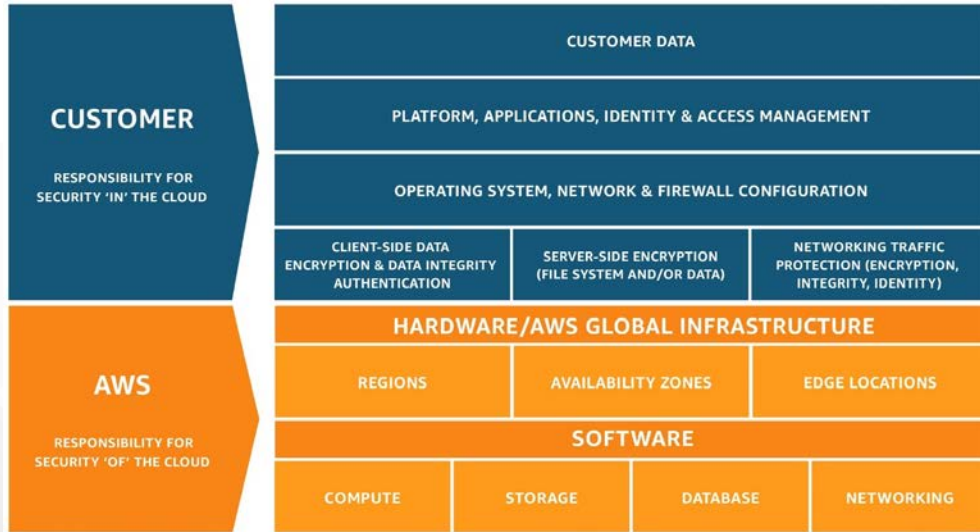
Why AWS? Why now? Compliance

 <https://aws.amazon.com/compliance/services-in-scope/>

 SOC 1-3, PCI, ISO, FedRAMP, HIPAA....

 FERPA is covered by extension

Why AWS? Why now? Security



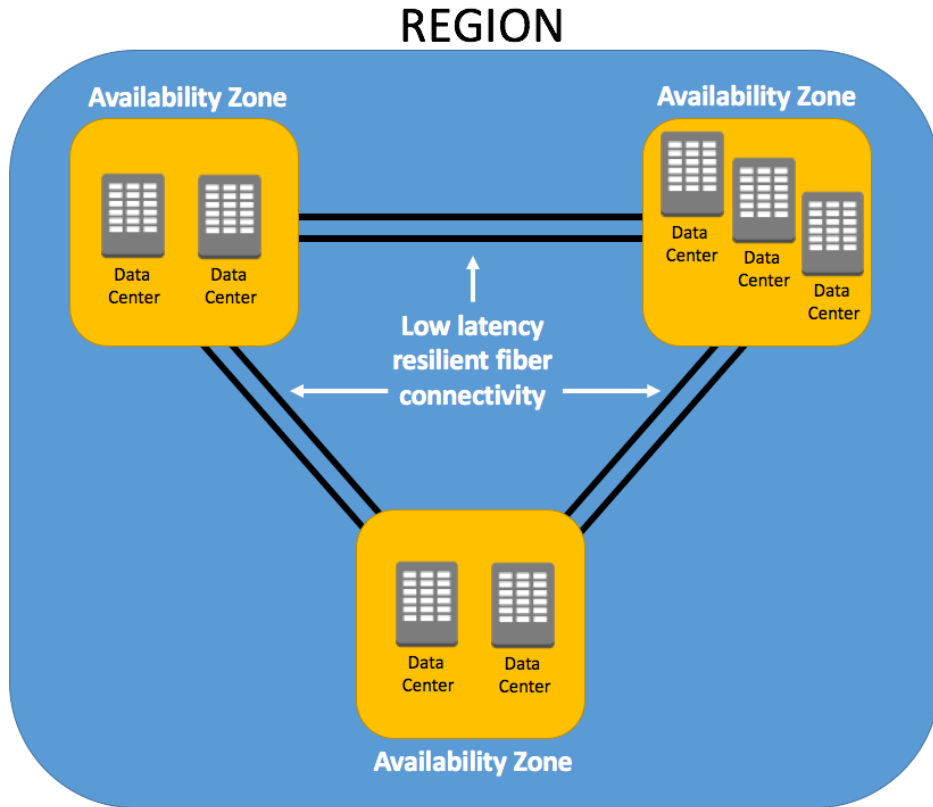
- ☼ AWS does not access content
- ☼ Data is encrypted in motion and at rest
- ☼ Data does not leave the US East N. Virginia Region
- ☼ Non-disclosure of information unless legally bound
- ☼ Independently validated security protections
- ☼ AWS ISO/FedRAMP compliance

AWS Regions

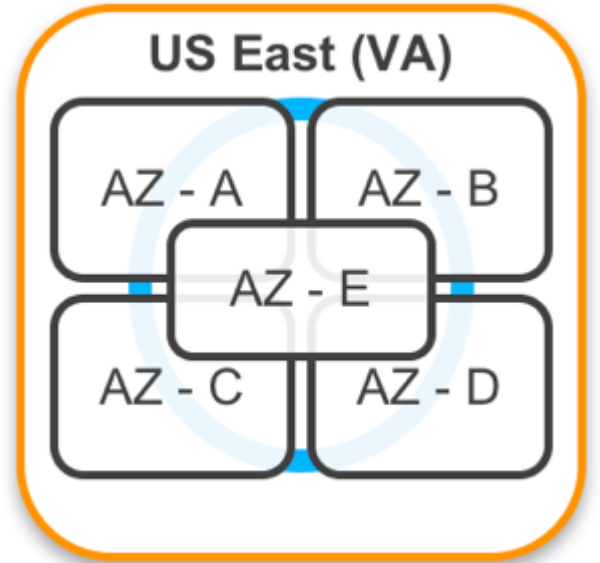
Reliability/Resiliency/Scalability



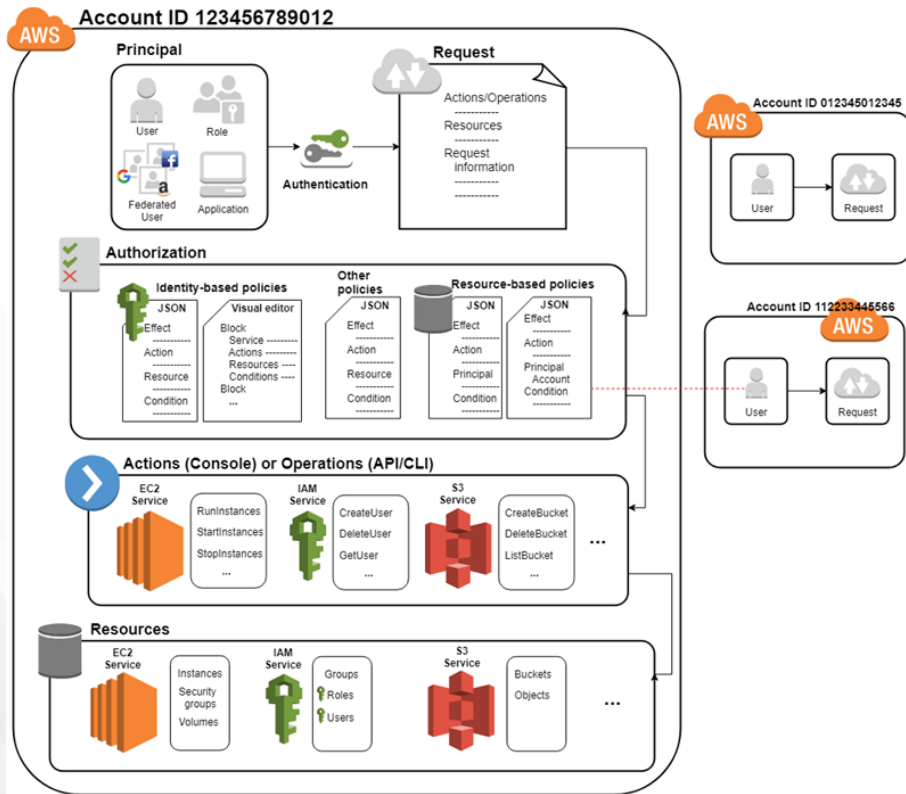
A region on AWS is comprised of Availability Zones, **each of which is a cluster of data centers.**



Reliability/Resiliency/Scalability

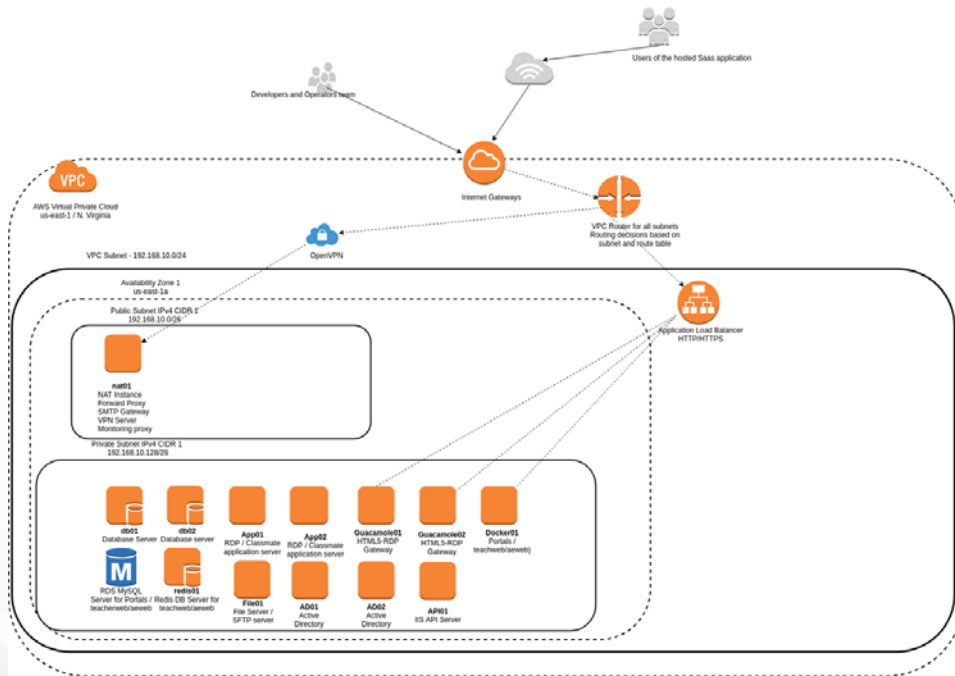


- Availability Zones on different flood plains
- Served by distinct public power utilities
- Multiple Tier 1 transit providers for network redundancy
- 25TB/sec connectivity between data centers



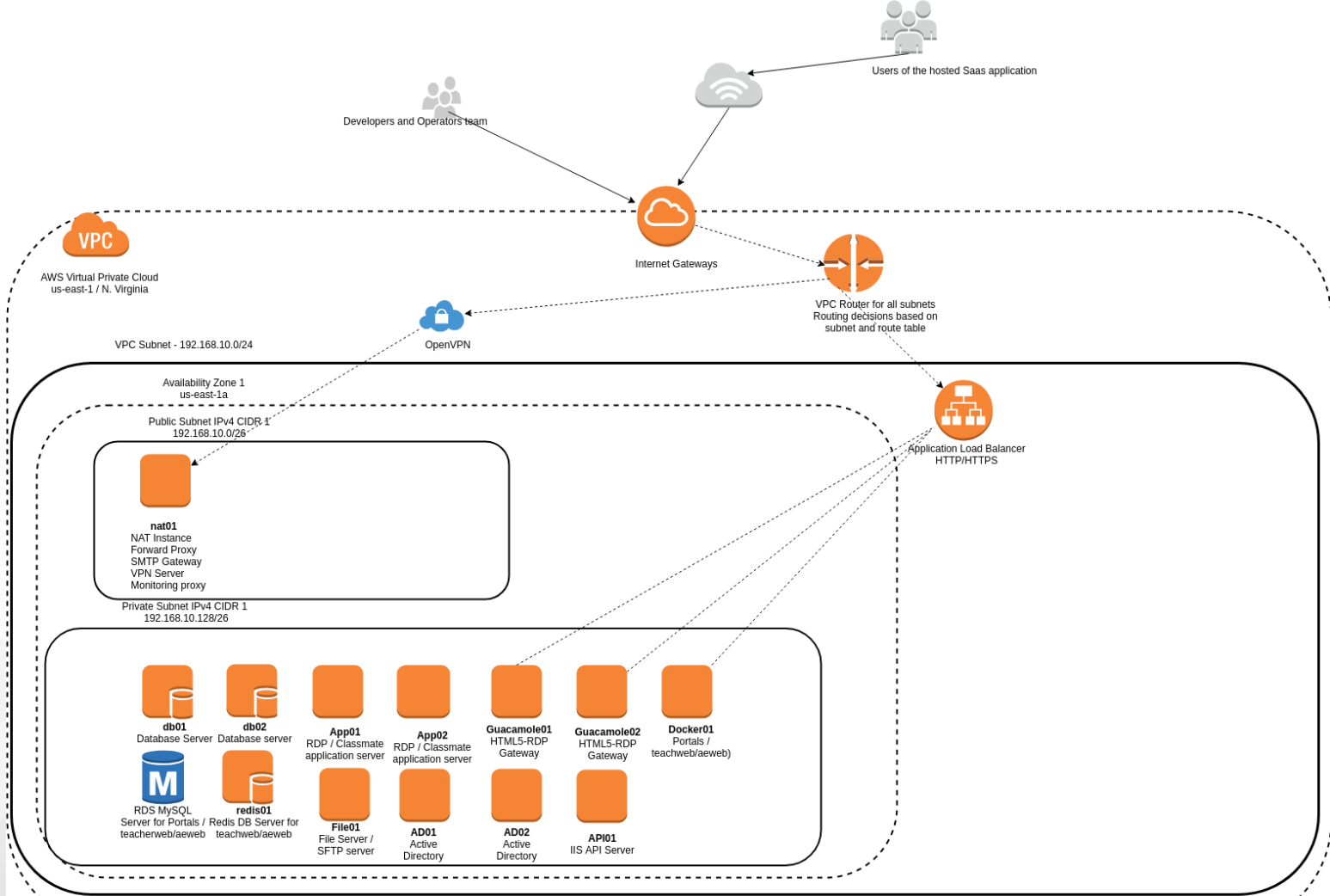
Key AWS Technologies

- AWS Organizations/Integrated Account Management (IAM)
- Key Management System (KMS) and CloudTrail auditing
- AWS service APIs
- Encrypted EBS volumes (SSD/SAN)
- Availability Zones



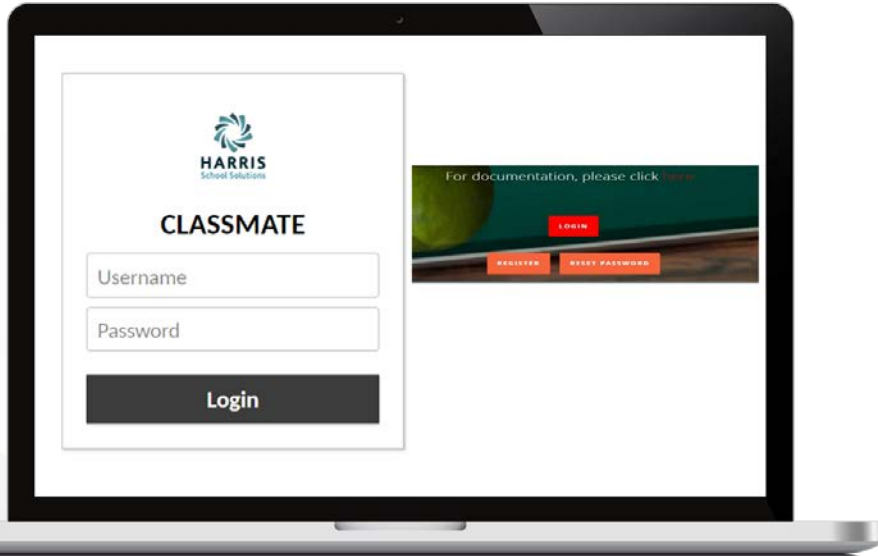
HES AWS Infrastructure Keys/Best Practices

- 🌀 Dedicated product accounts (via AWS Orgs/IAM)
- 🌀 Application and Development staff separated from access to the operating environment
- 🌀 Scripted infrastructure automation using Terraform (network) & Ansible (host configuration) to AWS APIs
- 🌀 Where possible recipes captured in docker
- 🌀 VPC perimeter/network firewall/ App Load Balancer (all ingress/egress controlled via OpenVPN & Forward Proxy)
- 🌀 Each VM wrapped in an individual host firewall
- 🌀 Stack hardened from OS on up at each layer (ex. TLS 1.2 for SSL)
- 🌀 Single point of entry for users via CM Gateway
- 🌀 Data sent to third parties controlled through 3 layers (Host Firewall then Edge Firewall then Forward Proxy)



ClassMate Gateway

- ❁ One secure, browser-based access method to manage for all users
- ❁ Mobile device support
- ❁ Self-service pw resets
- ❁ Transition transparent to teachers/users already on Gateway
- ❁ Downloading reports, printing and copying & pasting via Options Panel
- ❁ LaunchPad and M: Drive access (“Desktop”)
- ❁ Local drive uploads/downloads (G is for Guacamole)
- ❁ Crystal Reporting access



FERPA & NYED Law Section 2-d

Limit access

- ✓ Single access point for users (CM Gateway)
- ✓ CM Admin controls Username/PW management (discretionary policy w/multifactor authentication option)
- ✓ Application/Dev staff limited access (IAM/CloudTrail, VPN)
- ✓ Only Ops Team has access to infrastructure/servers

Only use data for authorized purposes

- ✓ HES Privacy Policy and Contracts, governed by HSS-Information Security Plan

Do not disclose PII without prior written consent or under legal order/statute with notice to LEA

- ✓ HES Privacy Policy, Contracts and AWS Terms comply

Maintain reasonable administrative, technical and physical safeguards

- ✓ Leveraging AWS best of breed tools (IAM, KMS, volume encryption)
- ✓ Physical environment is as secure as it gets (ISO, FedRAMP, SOC 3)
- ✓ HES infrastructure/AWS API scripting governs consistent and automated security control
- ✓ Staff receive annual FERPA training/encrypted drives/device management

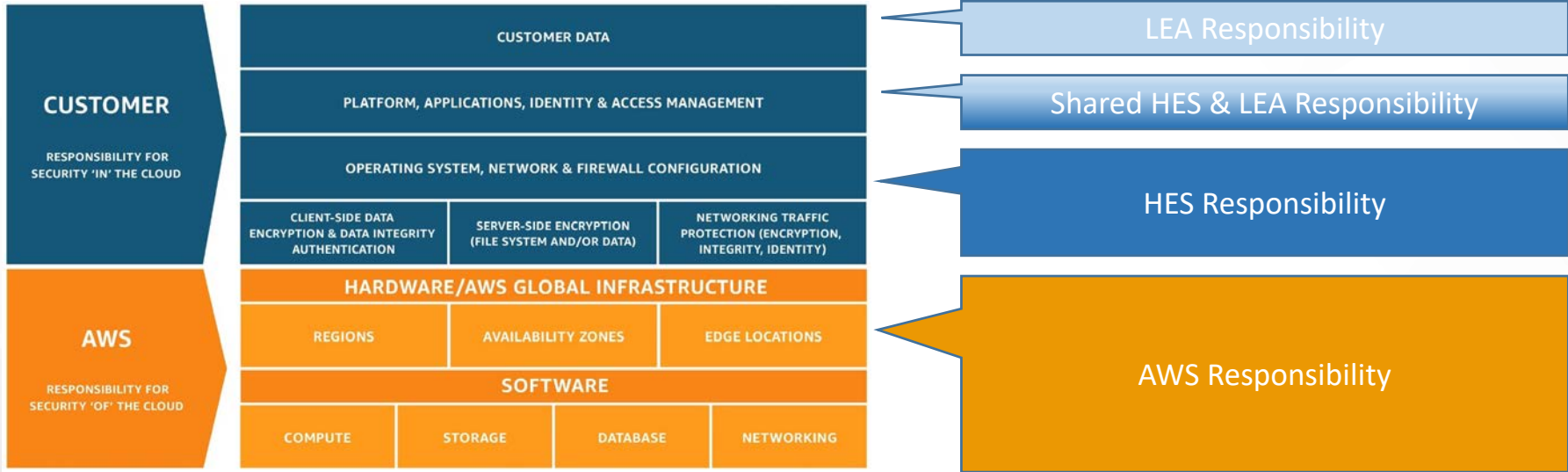
Use encryption while data is in motion or in custody

- ✓ TLS 1.2 for SSL and Encryption at Rest via EBS/SAN volume encryption
- ✓ MFT solution and 3-layer egress control/encryption for sharing data files

Breach notification protocol

- ✓ Detailed in HSS - Information Security Plan

ClassMate Security Responsibility Matrix



Cutover Methodology

Prior to cutover:

- HES copies production db to AWS for validation testing (live site still in LVQ)
- HES completes internal testing checks
- HES Requests client validation/sends checklist
- CTC/AE client validates checklist
- Issue resolution as needed
- Schedule production cutover

Final cutover:

- Stop access to LVQ production
- Copy db to AWS, complete internal testing
- Release site to CTC/AE client for final validation
- CTC/AE client notifies users of go-live
- HES staff on watch next day

Cutover Checklist

- ✓ Validate sample logins from all locations
- ✓ Validate record entry, editing, saving
 - ✓ ClassMate Admin functions
 - ✓ Teacher Web/Teacher client
 - ✓ Student, Parent, District portals
- ✓ Run daily reports and other critical reports
- ✓ Validate printing and saving to local machines
- ✓ Validate Crystal Reporting connections/running/saving edits
- ✓ Validate connection to Joomla and edits
- ✓ Test exports for third party systems
- ✓ Cleanup old CM accounts from prior years & populate email address
- ✓ Notify users of what to expect

THANK YOU!

Any questions?