SIG | CYBER

Navigating Higher Education Cybersecurity Compliance in AWS

PRESENTED BY:

Gabriel Tocci, ***SIG*** *Senior Consultant, Cloud Architect*
Patrick Frontiera, ***AWS*** *Campus & IT Operations*
Josh Badal, ***AWS*** *Campus & IT Operations*

Meet the Host

Patrick Frontiera

AWS

Patrick Frontiera leads the Campus and IT Operations portfolio at Amazon Web Services. In this role, Patrick is responsible for ensuring that colleges and universities successfully use AWS to sustain and differentiate their institutions. Prior to his role at AWS, Patrick was the CIO at Loyola Marymount University, where he was responsible for ensuring that the academic technology, administrative computing, infrastructure technology, and user support teams provided services that enabled LMU's mission. Before joining higher education, Patrick was the Director of Software Development at a start-up company in Santa Barbara and an application developer at PeopleSoft, Inc.

Meet the Panelist

Gabriel Tocci

Sr. Consultant/Cloud Architect

Gabriel is a senior cloud architect with deep expertise in Amazon Web Services (AWS), Oracle Cloud (OCI), Kubernetes (K8s), Infrastructure as Code (IaC), Cybersecurity, and various HigherEd enterprise systems. He has been working in Higher Education for two decades finding new ways to leverage these technologies so colleges and universities can focus on their mission of improving student success/outcomes.

Meet the Panelist

Josh Badal

AWS

Josh Badal is a leader in Amazon Web Services' campus and IT operations portfolio. He oversees technical solutions architecture across the United States.

Prior to his current role, Josh had extensive experience as a technology consultant. He worked on hundreds of enterprise projects involving on-premises, hybrid, and cloud infrastructure, cybersecurity, networking, systems, migrations, automation, research & development, with responsibilities that included solutions architecture, professional services, and managed services.

AGENDA

01 Cybersecurity Compliance in Higher Education

02 AWS Cybersecurity Summary

03 AWS Cybersecurity Compliance Services

04 Panel Discussion

05 Q&A

01

Cybersecurity Compliance Landscape in Higher Education

Higher Education Compliance Landscape

291 # of possible compliance regimes for a higher education institution[1]

24 # of “Information Technology” and “Privacy and Cybersecurity”

Common Examples

Family Education Rights and Privacy Act (FERPA)
PCI DSS (Payment Card Industry Data Security Standard)
Health Insurance Portability and Accountability Act (HIPAA)
Health Information Technology for Economic and Clinical Health (HITECH)
International Traffic in Arms Regulations (ITAR)
Federal Information Security Management Act (FISMA)

[1] Higher Education Compliance Alliance: https://www.higheredcompliance.org/compliance-programs/

What is the FTC Safeguards Rule

Enforced by the Federal Trade Commission

The safeguards rule requires financial institutions to maintain a documented information security program to protect customer information, and the recent changes expand on that requirement. The safeguards rule applies to customer information collected or maintained by financial institutions, and while it may seem out of place, **the FTC has deemed institutions of higher learning a non banking financial institution.**

In 2022, the Student Aid Internet Gateway Agreement required compliance with the expanded Safeguards Rule

Established in 2003 as part of the Gramm-Leach-Blilely (GLBA) financial modernization act to require financial institutions to document how they handle sensitive information

FTC Safeguards Rule Reporting Checklist

1 Designate or hire a "qualified individual" to oversee the cybersecurity program

2 Conduct a written risk assessment, including details about risk criteria and how the cybersecurity program will address and mitigate risks

3 Conduct additional periodic risk assessments

4 Implement role-based access to student information on a need-to-know basis

5 Identify and manage data, personal devices, systems and facilities

6 Document the data and system inventory of all the information the College collects, stores, and transmits

7 Encrypt all student information in transit and at rest

8 Adopt secure development practices for in-house developed applications

9 Enforce multi-factor authentication (MFA) for all systems containing sensitive student information

10 Develop documented retention and disposal procedures for all student information

11 Establish change management procedures for modifying information systems

12 Implement policies, procedures and controls to monitor and log activity of authorized/unauthorized users

13 Perform annual penetration testing, twice-yearly vulnerability assessments, and periodic vendor risk assessments

14 Perform end user awareness and internal information security training to employees

15 Document a written incident response plan including goals, communications plan, processes, and roles/responsibilities

16 Provide annual reports to my board of trustees on compliance and cyber hygiene status

Why must Colleges and Universities comply?

Each institution that participates in the Title IV programs has agreed in its Program Participation Agreement (PPA) to comply with the GLBA Safeguards Rule under 16 C.F.R. Part 314

Institutions and servicers also sign the Student Aid Internet Gateway (SAIG) Enrollment Agreement, which states that they will ensure that all Federal Student Aid applicant information is protected from access by, or disclosure to, unauthorized personnel, and that they are aware of and will comply with all of the requirements to protect and secure data obtained from the Department's systems for the purposes of administering the Title IV programs.

What is NIST 800-171

Born from the Federal Information Security Management Act of 2002 (FISMA) moderate level, NIST 800-171 codifies requirements for non-Federal systems to store, process, and transmit CUI

Pending rule from Federal Student Aid (FSA) that imposes requirements on storage, processing, or transmitting of Controlled Unclassified Information (CUI) or provide security protection for such systems

Security control categories:

Access Control

Awareness and Training

Audit and Accountability

Configuration Management

Contingency Planning

Identification and Authentication

Incident Response

Maintenance

Media Protection

Personnel Security

Physical Protection

Risk Assessment

Security Assessment and Monitoring

System and Communications Protection

System and Information Integrity

Planning

System and Services Acquisition

Supply Chain Risk Management

Why should institutions ready themselves?

While it is uncertain exactly when Federal Student Aid will require NIST 800-171 compliance, to the extent that it aligns with the Safeguards Rule, it may be in your institution’s interest to evaluate gap between Safeguards Rule and NIST 800-171

NIST 800-171 compliance is ***foundational*** to emerging compliance regimes like Cybersecurity Maturity Model Certification (CMMC), a requirement for institutions seeking to contract with the Department of Defense

Challenges

Ever-changing tsunami of regimes

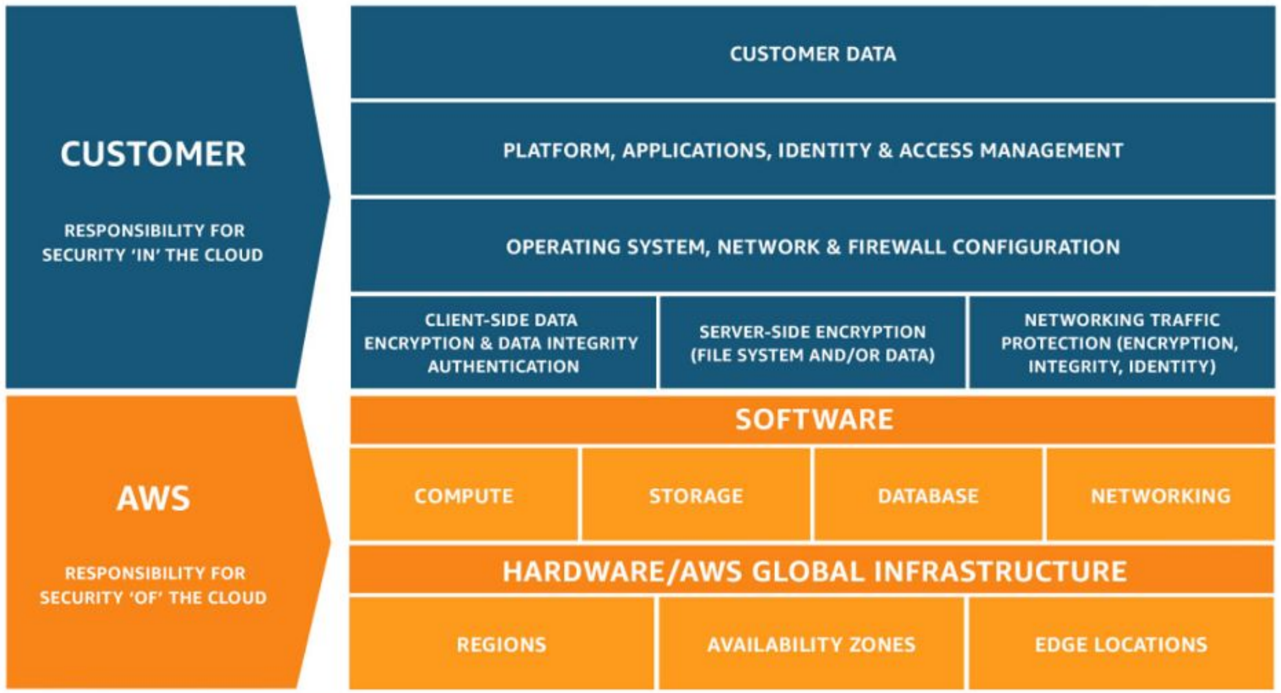
Applicability and gaps

Resources / Opportunity cost

02

How AWS and SIG can help

AWS’s Shared Responsibility Model



CUSTOMER

RESPONSIBILITY FOR SECURITY ‘IN’ THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY ‘OF’ THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

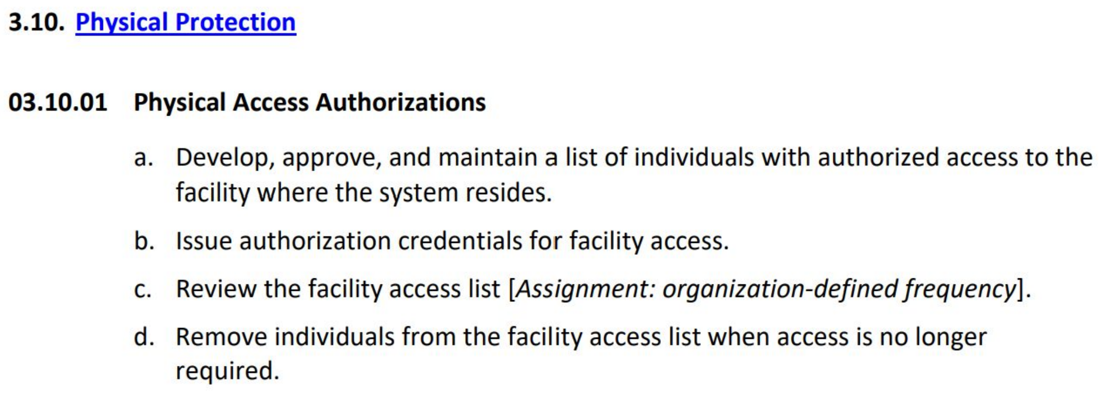
HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

NIST 800-171 control example



3.10. Physical Protection

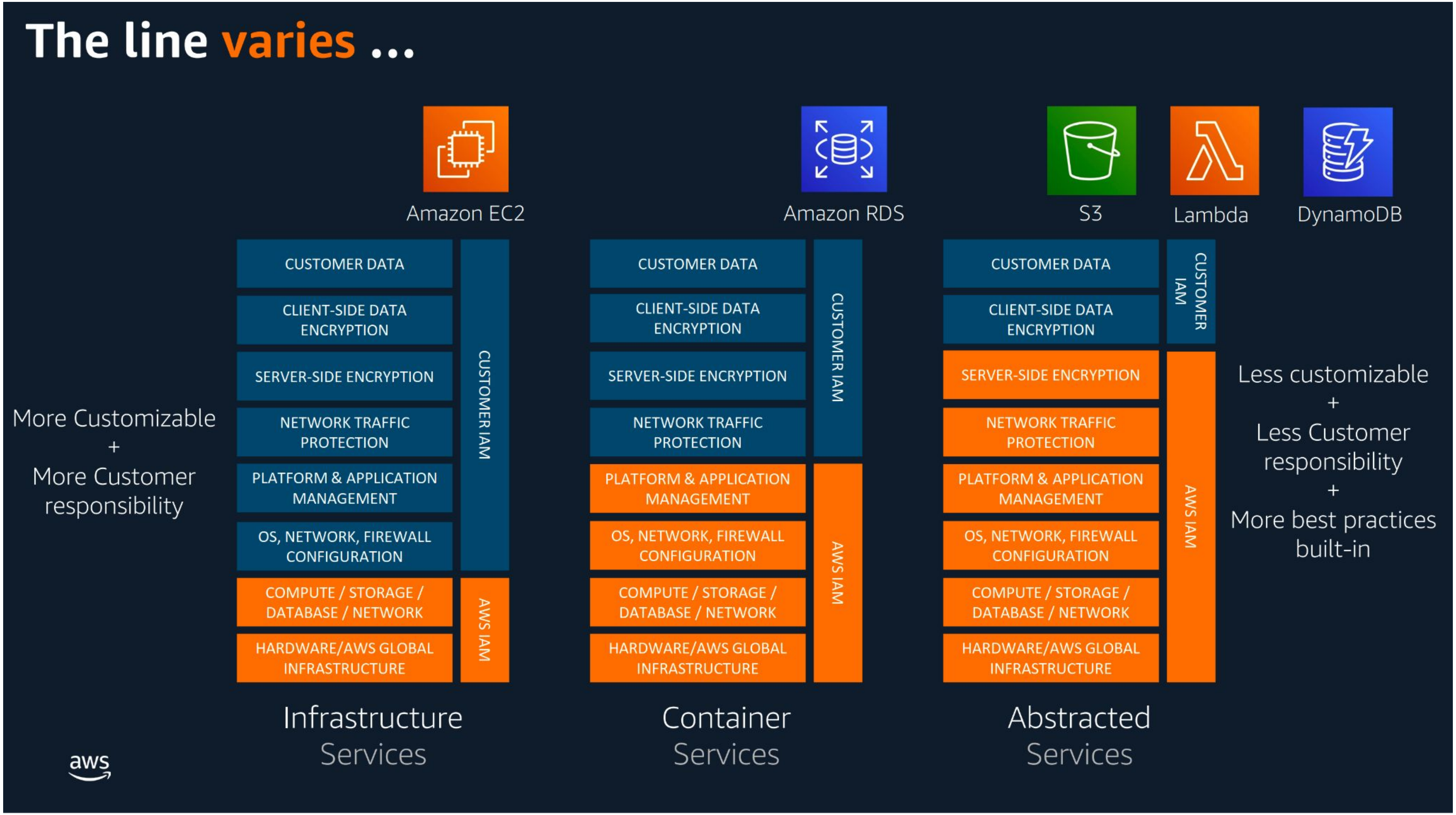
03.10.01 Physical Access Authorizations

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.

b. Issue authorization credentials for facility access.

c. Review the facility access list [*Assignment: organization-defined frequency*].

d. Remove individuals from the facility access list when access is no longer required.



The line varies …

Amazon EC2

CUSTOMER DATA	CUSTOMER IAM
CLIENT-SIDE DATA ENCRYPTION	
SERVER-SIDE ENCRYPTION	
NETWORK TRAFFIC PROTECTION	
PLATFORM & APPLICATION MANAGEMENT	
OS, NETWORK, FIREWALL CONFIGURATION	
COMPUTE / STORAGE / DATABASE / NETWORK	AWS IAM
HARDWARE/AWS GLOBAL INFRASTRUCTURE	

Infrastructure Services

Amazon RDS

CUSTOMER DATA	CUSTOMER IAM
CLIENT-SIDE DATA ENCRYPTION	
SERVER-SIDE ENCRYPTION	
NETWORK TRAFFIC PROTECTION	
PLATFORM & APPLICATION MANAGEMENT	AWS IAM
OS, NETWORK, FIREWALL CONFIGURATION	
COMPUTE / STORAGE / DATABASE / NETWORK	
HARDWARE/AWS GLOBAL INFRASTRUCTURE	

Container Services

S3

Lambda

DynamoDB

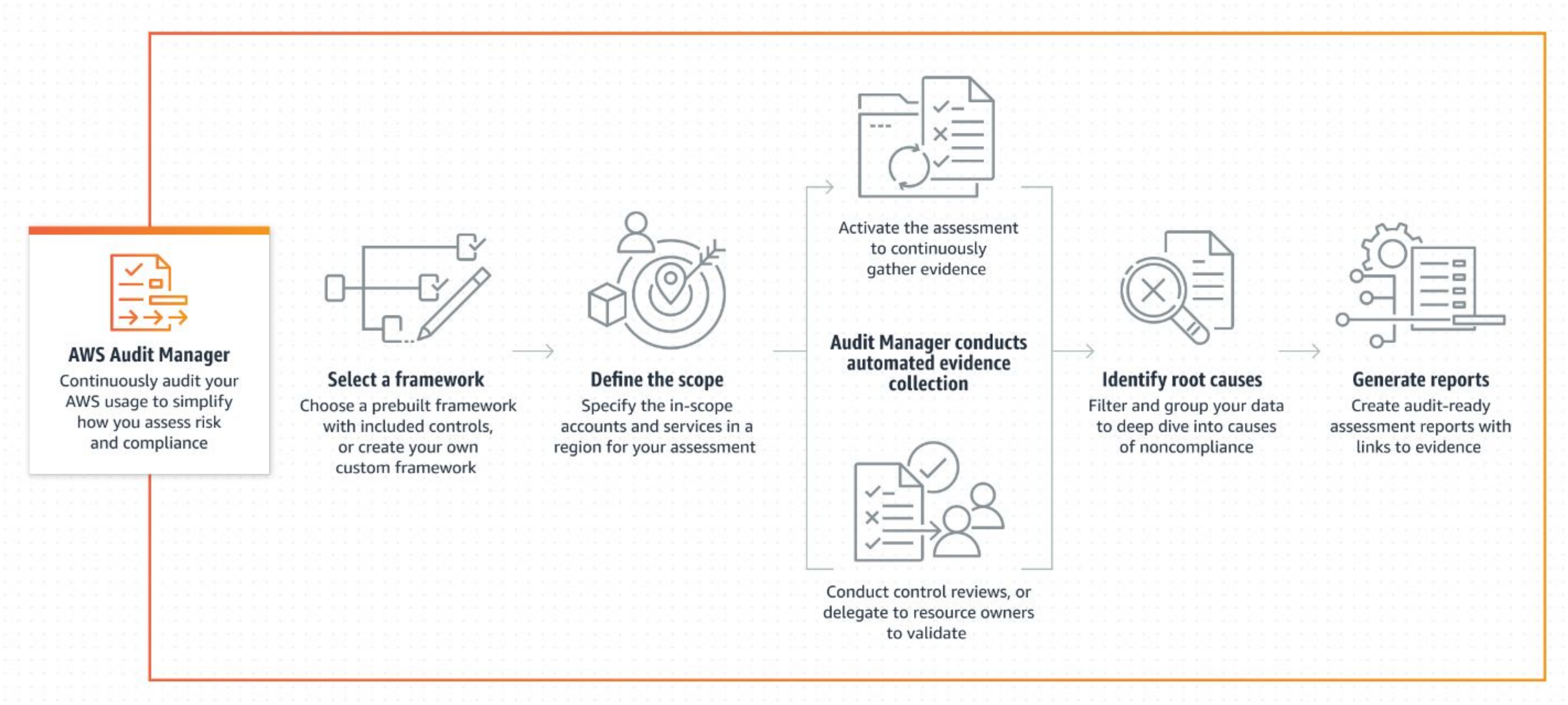
CUSTOMER DATA	CUSTOMER IAM
CLIENT-SIDE DATA ENCRYPTION	
SERVER-SIDE ENCRYPTION	AWS IAM
NETWORK TRAFFIC PROTECTION	
PLATFORM & APPLICATION MANAGEMENT	
OS, NETWORK, FIREWALL CONFIGURATION	
COMPUTE / STORAGE / DATABASE / NETWORK	
HARDWARE/AWS GLOBAL INFRASTRUCTURE	

Abstracted Services

More Customizable
+
More Customer responsibility

Less customizable
+
Less Customer responsibility
+
More best practices built-in

AWS Audit Manager



AWS Audit Manager
Continuously audit your AWS usage to simplify how you assess risk and compliance

Select a framework
Choose a prebuilt framework with included controls, or create your own custom framework

Define the scope
Specify the in-scope accounts and services in a region for your assessment

Activate the assessment to continuously gather evidence

Audit Manager conducts automated evidence collection

Conduct control reviews, or delegate to resource owners to validate

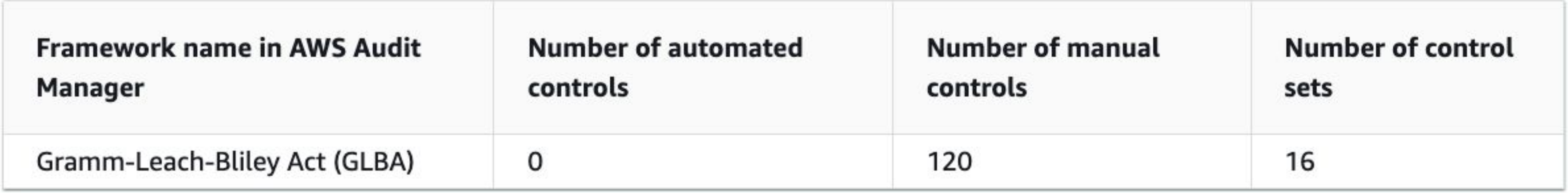
Identify root causes
Filter and group your data to deep dive into causes of noncompliance

Generate reports
Create audit-ready assessment reports with links to evidence

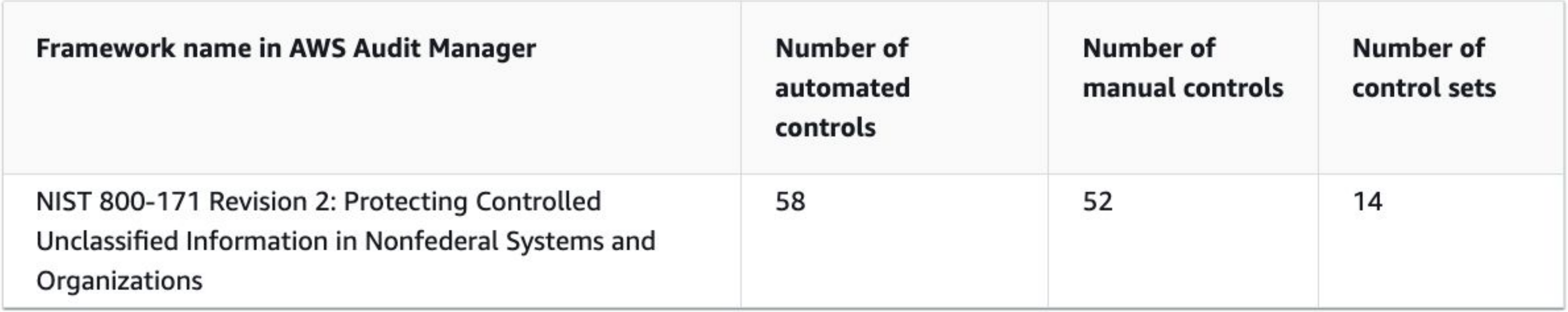
AWS Audit Manager

- ACSC Essential Eight
- ACSC ISM 02 March 2023
- AWS Audit Manager Sample Framework
- AWS Control Tower Guardrails
- AWS generative AI best practices framework v2
- AWS License Manager
- AWS Foundational Security Best Practices
- AWS Operational Best Practices
- AWS Well Architected Framework WAF v10
- CCCS Medium Cloud Control
- CIS AWS Benchmark v1.2.0
- CIS AWS Benchmark v1.3.0
- CIS AWS Benchmark v1.4.0
- CIS Controls v7.1, IG1
- CIS Critical Security Controls version 8.0, IG1
- FedRAMP Security Baseline Controls r4
- GDPR 2016
- Gramm-Leach-Bliley Act
- Title 21 CFR Part 11
- EU GMP Annex 11, v1
- HIPAA Security Rule: Feb 2003
- HIPAA Omnibus Final Rule
- ISO/IEC 27001:2013 Annex A
- NIST SP 800-53 Rev 5
- NIST Cybersecurity Framework v1.1
- NIST SP 800-171 Rev 2
- PCI DSS V3.2.1
- PCI DSS V4.0
- SSAE-18 SOC 2

AWS Audit Manager

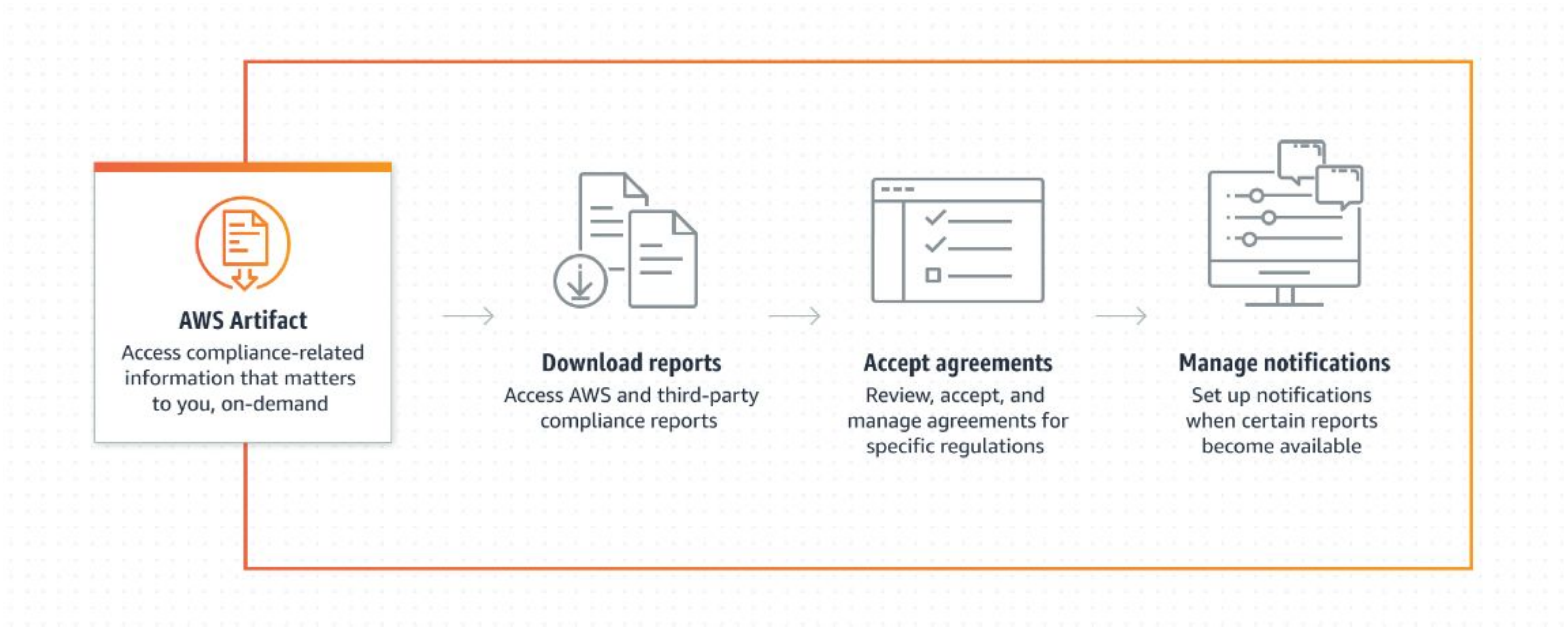


Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
Gramm-Leach-Bliley Act (GLBA)	0	120	16



Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets
NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	58	52	14

AWS Artifact



AWS Artifact
Access compliance-related information that matters to you, on-demand

→

Download reports
Access AWS and third-party compliance reports

→

Accept agreements
Review, accept, and manage agreements for specific regulations

→

Manage notifications
Set up notifications when certain reports become available

PANEL DISCUSSION

WWW.SIGCORP.COM

QUESTIONS?

WWW.SIGCORP.COM

Contact

Gabriel Tocci
Sr. Consultant / Cloud Architect
tocci@sigcorp.com

Brian Kirk
Executive Vice President, Cybersecurity Services
kirk@sigcorp.com

Kyle Bork
Director of Business Development, Cybersecurity
bork@sigcorp.com

in /strata-information-group

@SIGCorpLIVE

sigcorp.com