BPM

Auditing and the Cloud
The Responsibilities

Presented by Sarah A. Lynn, BPM IT Security Advisory Managing Partner

July 8, 2020

BPM

Sarah A. Lynn

salynn@bpmcpa.com

P 408.333.9824

Ms. Lynn has over 30 years of experience in IT, Information Security, Compliance, Risk Management, Advisory/Audit Prep, Business Continuity/DR, Project Management, Operations, and Technology Engineering. She has served on ISACA Partner Panels, the Embrane Technical Advisory Board, A10 Technical Advisory Board, Cisco CIO Advisory Board, Astia Angels Advisor, and was a 2014 ISC2 InfoSec Rockstar nominee for the 4th Annual Americas Information Security Leadership Achievements Program (AM-ISLA) for South, Central, and North American regions.

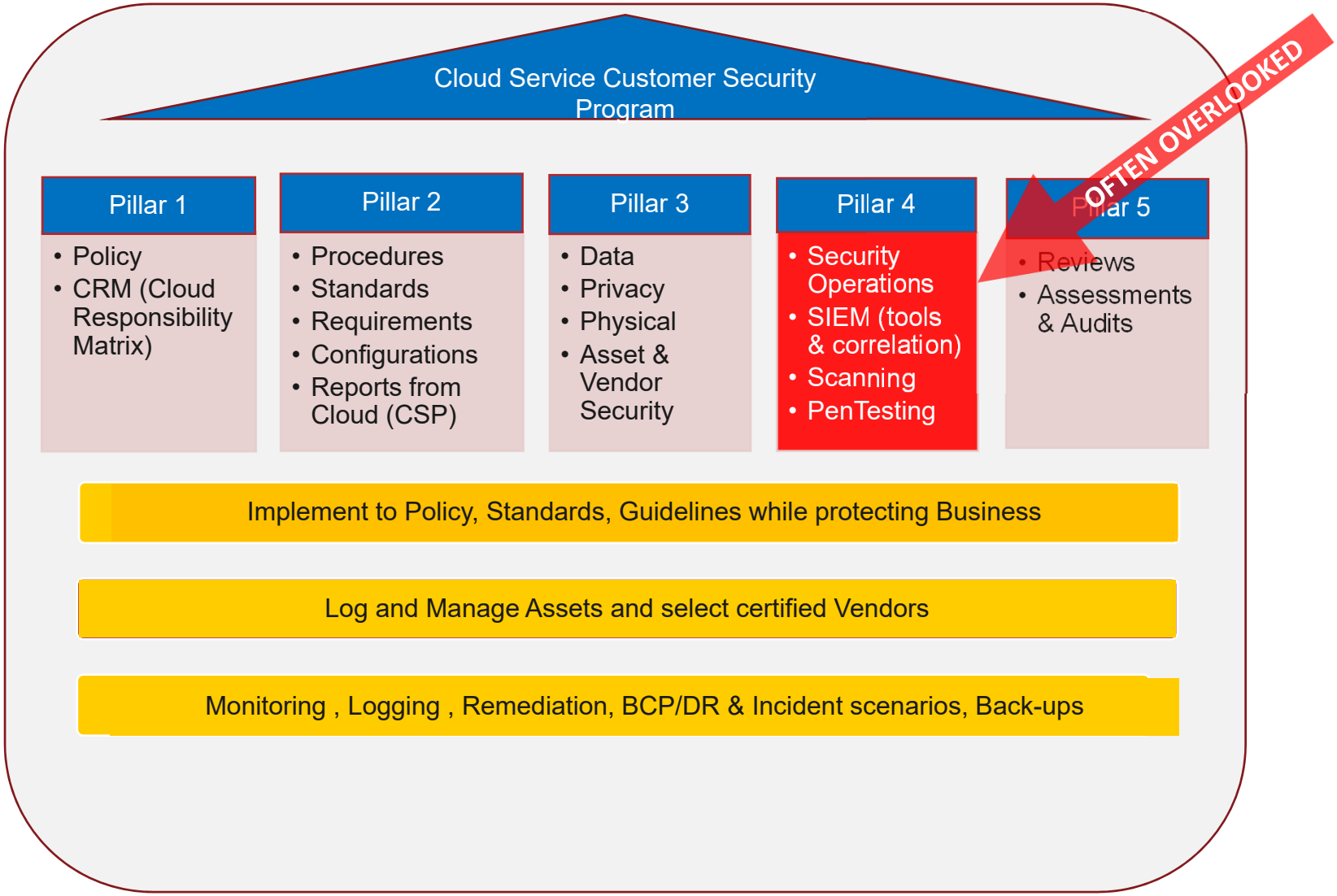
Agenda

- Learn About
  - Cloud Service Provider - host
  - Cloud Service Provider - SaaS
  - Cloud Service Customer – to host
  - Cloud Service Customer – to SaaS product
- Demonstrate
  - How responsibility works
  - Who’s responsible
  - What happens when that doesn’t work/corner cases
  - How to review CSPs

Quick Definitions

- Cloud Service Provider – Host (a location that has servers and network instead of your company having it on their premises or “on prem”)
- Cloud Service Provider – SaaS (software like Adobe on-line is SaaS – software as a service)
- Cloud Service Provider – PaaS (platform as a service is PaaS and Microsoft Office 365 offering email, calendar, apps, sharepoint, storage, encryption in the cloud, etc.)
- Cloud Service Provider – IaaS (infrastructure as a service is IaaS and some companies like RackSpace offer where you can build your own network, systems, applications and the CSP runs them or “shares responsibility” of maintaining them)
- Cloud Service Customer – Your company is the Customer unless you own a technology too (you could be both but likely not at the same time)

Cloud Security Programs can be Shared



Basics of Cloud Responsibilities

- **Why we assign responsibilities (for security and audit purposes):**
  - What team/group/company owns the control?
  - Who shall we talk to in order to see the strength of a control or control set?
  - When a control is not met, who owns correcting it?

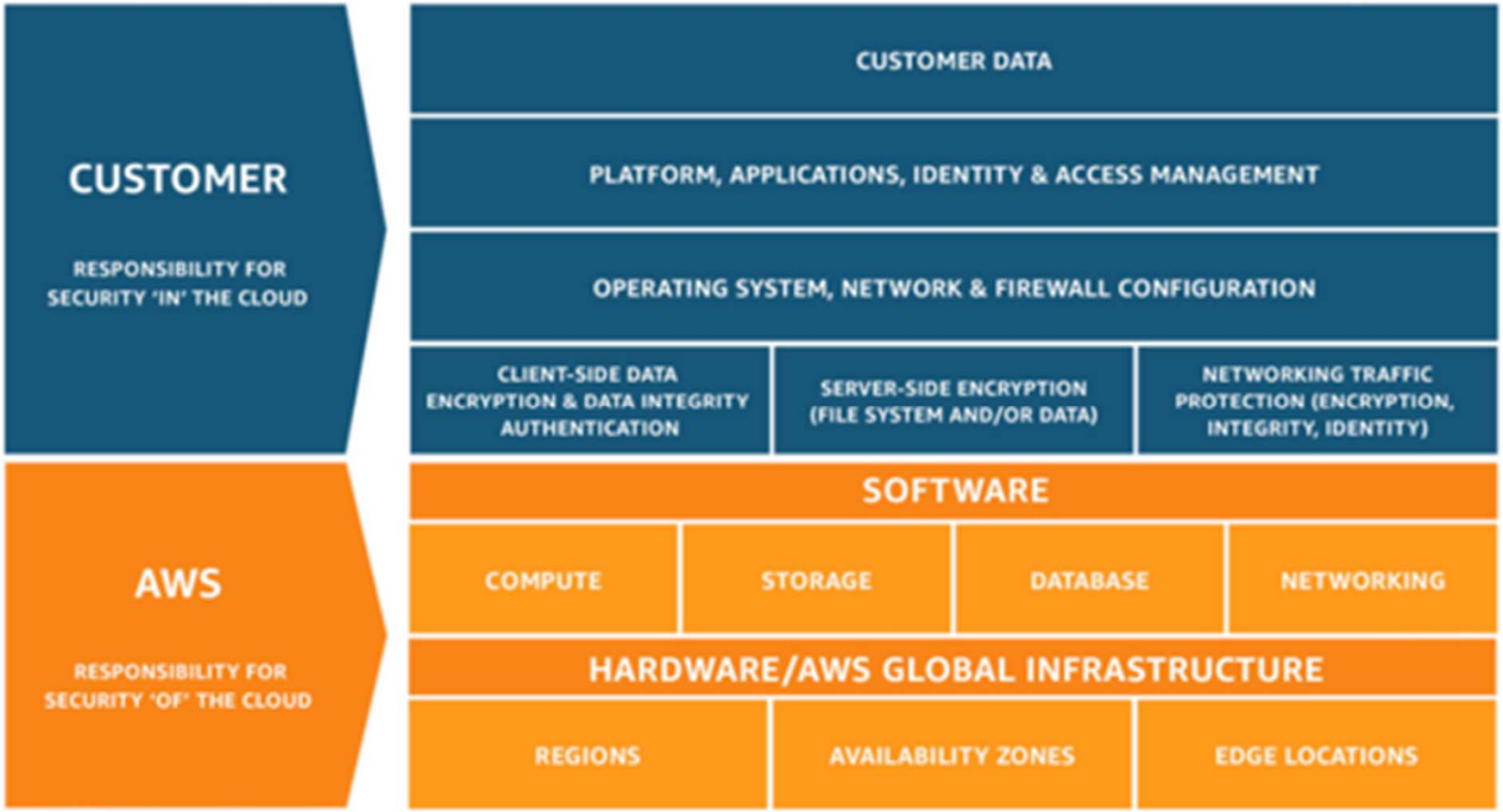
The Myth

“If my company deploys our products or services to another host’s platform (e.g., AWS, Rackspace, or even a data processor host), we are no longer responsible if it is breached or not secure.”

Cloud Service Providers

SaaS/PaaS (Software/Platform)

Ex. AWS- Amazon Web Services



Cloud Service Providers

Ex. AWS- Amazon Web Services

AWS responsibility "Security of the Cloud" - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility "Security in the Cloud" – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, services such as Amazon Elastic Compute Cloud (Amazon

Auditor & Customer (system owner) should request AWS (3rd party's) audit of their security for all of these controls.

Auditor & Customer (system owner) should review all compliance controls and delineate what owners need to do.

BPM

Cloud Service Providers

Ex. AWS- Amazon Web Services

Shared Controls – Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:

- Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
- Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.

Auditor & Customer (system owner) should request AWS (3rd party's) audit of their security for all of these controls.

Auditor & Customer (system owner) should review all compliance controls and delineate what owners need to do.

BPM

Cloud Service Providers

NIST Controls owned by AWS

Inherited Controls – Controls which a customer fully inherits from AWS.

- Physical and Environmental controls

Control	Control Statement	Assessor Response
PE-01	**The organization:**	
PE-01a	*a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:* *1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and* *2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and*	**Inherited**
PE-02	**The organization:**	
PE-02a	*a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;*	**Inherited**

Auditor & Customer (system owner) should request AWS (3rd party's) audit of their security for all of these controls.

If there are findings, Auditor and Customer (system owner) have right to ask for fix time commitment.

Cloud Service Providers

NIST Controls owned by AWS (cont.)

Control	Control Statement	Assessor Response
PE-01	**The organization:**	
PE-01a	*a. Develops, documents, and disseminates to [%Assignment: organization-defined personnel or roles%]:* *1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and* *2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and*	**Inherited**
PE-02	**The organization:**	
PE-02a	*a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;*	**Inherited**

Control	Control Statement	Assessor Response
PE-03	**The organization:**	
PE-03a	*a. Enforces physical access authorizations at [%Assignment: organization-defined entry/exit points to the facility where the information system resides%] by;* *1. Verifying individual access authorizations before granting access to the facility; and* *2. Controlling ingress/egress to the facility using [%Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards%];*	**Inherited**
PE-03b	*b. Maintains physical access audit logs for [%Assignment: organization-defined entry/exit points%];*	**Inherited**
PE-03c	*c. Provides [%Assignment: organization-defined security safeguards%] to control access to areas within the facility officially designated as publicly accessible;*	**Inherited**
PE-03d	*d. Escorts visitors and monitors visitor activity [%Assignment: organization-defined circumstances requiring visitor escorts and monitoring%];*	**Inherited**
PE-03e	*e. Secures keys, combinations, and other physical access devices;*	**Inherited**

Cloud Service Providers

NIST Controls owned by AWS (cont.)

Control	Control Statement	Assessor Response
PE-04	The organization controls physical access to [%Assignment: organization-defined information system distribution and transmission lines%] within organizational facilities using [%Assignment: organization-defined security safeguards%].	Inherited
PE-05	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Inherited
PE-06	The organization:	
PE-06 (01)	The organization monitors physical intrusion alarms and surveillance equipment.	Inherited
PE-08	The organization:	
PE-08a	*a. Maintains visitor access records to the facility where the information system resides for [%Assignment: organization-defined time period%]; and*	Inherited
PE-09	The organization protects power equipment and power cabling for the information system from damage and destruction.	Inherited
PE-10	The organization:	
PE-11	The organization provides a short-term uninterruptible power supply to facilitate [%Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power%] in the event of a primary power source loss.	Inherited

Control	Control Statement	Assessor Response
PE-12	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	Inherited
PE-13	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	Inherited
PE-14	The organization:	
PE-15	The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	Inherited
PE-16	The organization authorizes, monitors, and controls [%Assignment: organization-defined types of information system components%] entering and exiting the facility and maintains records of those items.	Inherited
PE-17	The organization:	
PE-17a	*a. Employs [%Assignment: organization-defined security controls%] at alternate work sites;*	Inherited

BPM

Cloud Service Providers

ISO 2700x Controls owned by AWS

Section 11 - Physical and Environmental Security	
11.1	***Secure Areas***
11.1.1	Is a physical security perimeter defined and used to protect areas that contain either sensitive information or critical information and information processing facilities?
11.1.2	Are all secure areas protected by appropriate entry controls to ensure that only authorized personnel are allowed to access?
11.1.4	Do your facilities have physical protection against natural disasters, malicious attacks, or potential accidents? Please describe.
11.1.6	Are visitor access points, such as delivery, loading areas, and lobbies, controlled? Are these points isolated from information processing facilities to avoid unauthorized access?

Auditor & Customer (system owner) should request AWS (3rd party's) audit of their security for all of these controls.

If there are findings, Auditor and Customer (system owner) have right to ask for fix time commitment.

Cloud Service Providers

ISO 2700x Controls owned by AWS (cont.)

11.2	***Equipment***
11.2.1	Is equipment sited and protected to reduce the risks from environmental threats and hazards, as well as opportunities for unauthorized access?
11.2.2	Is equipment protected from power failure and other disruptions caused for failures in supporting utilities?
11.2.3	Are power and telecommunications cables that are carrying data or supporting information services protected from interception, interference, or damage?
11.2.4	Is all equipment correctly maintained to ensure continued availability and integrity?
11.2.5	Does your organization require authorization before an equipment, information, or software is taken off-site?

Auditor & Customer (system owner) should request AWS (3rd party's) audit of their security for all of these controls.

If there are findings, Auditor and Customer (system owner) have right to ask for fix time commitment.

Cloud Service Providers – Host

Rackspace.gov Example

Rackspace.gov has similar responsibilities as AWS and some additional. These are inherited or shared.

CP-06	The organization:	
CP-06 (01)	The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	Inherited
CP-06 (03)	The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Inherited

Auditor & Customer (system owner) should request RGC (3rd party's) audit of their security for all of these controls.

Auditor & Customer (system owner) should review all compliance controls and delineate what owners need to do.

Cloud Service Providers - Host

Rackspace.gov Example (cont.)

Control	Control Statement	Assessor Response
CP-08	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [%Assignment: organization-defined information system operations%] for essential missions and business functions within [%Assignment: organization-defined time period%] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	Inherited
CP-08 (01)	The organization:	
CP-08 (01)b	*(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.*	Inherited

Auditor & Customer (system owner) should request RGC (3rd party's) audit of their security for all of these controls.

Auditor & Customer (system owner) should review all compliance controls and delineate what owners need to do.

Cloud Service Providers - Host

Rackspace.gov Example (cont.)

PS (Personnel Security) are shared since the screening may be required on Rackspace and Customer side.

Control	Control Statement	Assessor Response
IA-03	The information system uniquely identifies and authenticates [%Assignment: organization-defined specific and/or types of devices%] before establishing a [%Selection (one or more): local; remote; network%] connection.	Inherited
RA-02	The organization:	
RA-02a	*a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;*	Inherited
SI-08 (01)	The organization centrally manages spam protection mechanisms.	Inherited

Auditor & Customer (system owner) should request RGC (3rd party's) audit of their security for all of these controls.

Auditor & Customer (system owner) should review all compliance controls and delineate what owners need to do.

BPM

Cloud Service Customer (CSC)

System Owners

All AC (Access Control) controls are responsibility of CSC. The CSP may provide the method, but the CSC is responsible for utilizing. E.g., Multi-Factor authentication requirements and integration may be provided, but the CSC is responsible for implementing.

All CSC's are responsible for:

AT (Awareness and Training) controls

AU (Audit and Accountability) – extra assurance that CSP is maintaining their part and testing (through scanning and penetration testing that their controls & CSCs work)

CA (Security Assessments and Authorization) – extra assurance that assessments and authorization rules are tightly adhered to

Auditor & Customer (system owner) should request RGC (3rd party's) audit of their security for all of these controls.

Auditor & Customer (system owner) should review all compliance controls and delineate what owners need to do.

Cloud Service Customer (CSC)

System Owners (cont.)

All CSCs are additionally responsible for:

CM (Configuration Management) - shared configuration and automation and extra assurance that automation works without ability to have a human manipulate

CP (Contingency Planning) – assurance that high-availability only is not substituted for a back-up requirement and that tests are completed annually (CSP and CSC)

IA (Identification and Authentication) – testing that authentication tools work and identity can not be spoofed by utilizing the NIST-140-2 validation site

IR (Incident Response) – ensure additional scenarios for Cloud and Cloud breaches

Auditor & Customer (system owner) should request RGC (3rd party's) audit of their security for all of these controls.

Auditor & Customer (system owner) should review all compliance controls and delineate what owners need to do.

Cloud Service Customer (CSC)

System Owners (cont.)

All CSCs are additionally responsible for:

MA (Maintenance) – delineate the maintenance for CSC and that for CSP are being upheld

MP (Media Protection) – ensure all media protection is upheld even within or to multiple CSPs

PL (Planning) and RA (Risk Assessments) – ensure extra diligence, planning, and assessments are done prior to integrating with any CSP and on-going

SA (Systems Acquisition) – ensure by staging/test and review (like code review) that a process stays in place for Change and Modification

SC (Systems Communications) – ensure that communication and sharing of data stays secure between CSC and CSP

Auditor & Customer (system owner) should request RGC (3rd party's) audit of their security for all of these controls.

Auditor & Customer (system owner) should review all compliance controls and delineate what owners need to do.

Cloud Service Customer (CSC)

System Owners (cont.)

All CSCs are additionally responsible for:

SI (Systems Integrity) – ensure that integrity testing continues even while data is located at CSP – data is not modified

PM (Program Management) – ensure that every project between the CSC and CSP has standards for security and project management documented

Auditor & Customer (system owner) should request RGC (3rd party's) audit of their security for all of these controls.

Auditor & Customer (system owner) should review all compliance controls and delineate what owners need to do.

References

- https://www.nist.gov/document/csfsubcategories-sp80053mappingxlsx
- https://www.fedramp.gov/templates/
- https://www.iso.org/standard/43757.html

Thank You!

www.bpmcpa.com
408.333.9824