ISACA The Institute of Internal Auditors

GRC CONFERENCE 2019

Where Governance and Risk Management Align for Impact

Who is Responsible for the Security of Cloud-based Information Systems?

Dr. Sarbari Gupta

WHAT PERCENTAGE OF YOUR ORGANIZATIONAL INFORMATION SYSTEMS ARE IMPLEMENTED IN THE CLOUD?

Please open the conference app to participate

Polling Question

Choices:

a. 0%
b. 25%
c. 50%
d. 70%
e. 100%

Why are many Information Systems Migrating to Cloud?

- To comply with mandates such as “Cloud First!”
- To leverage the many benefits of the cloud
  - Hardware/Software Footprint Reduction
  - Scalability
  - Elasticity
  - Lower Cost
  - Improved Availability
  - Outsourced Security Responsibility

Who Secures Cloud Systems?

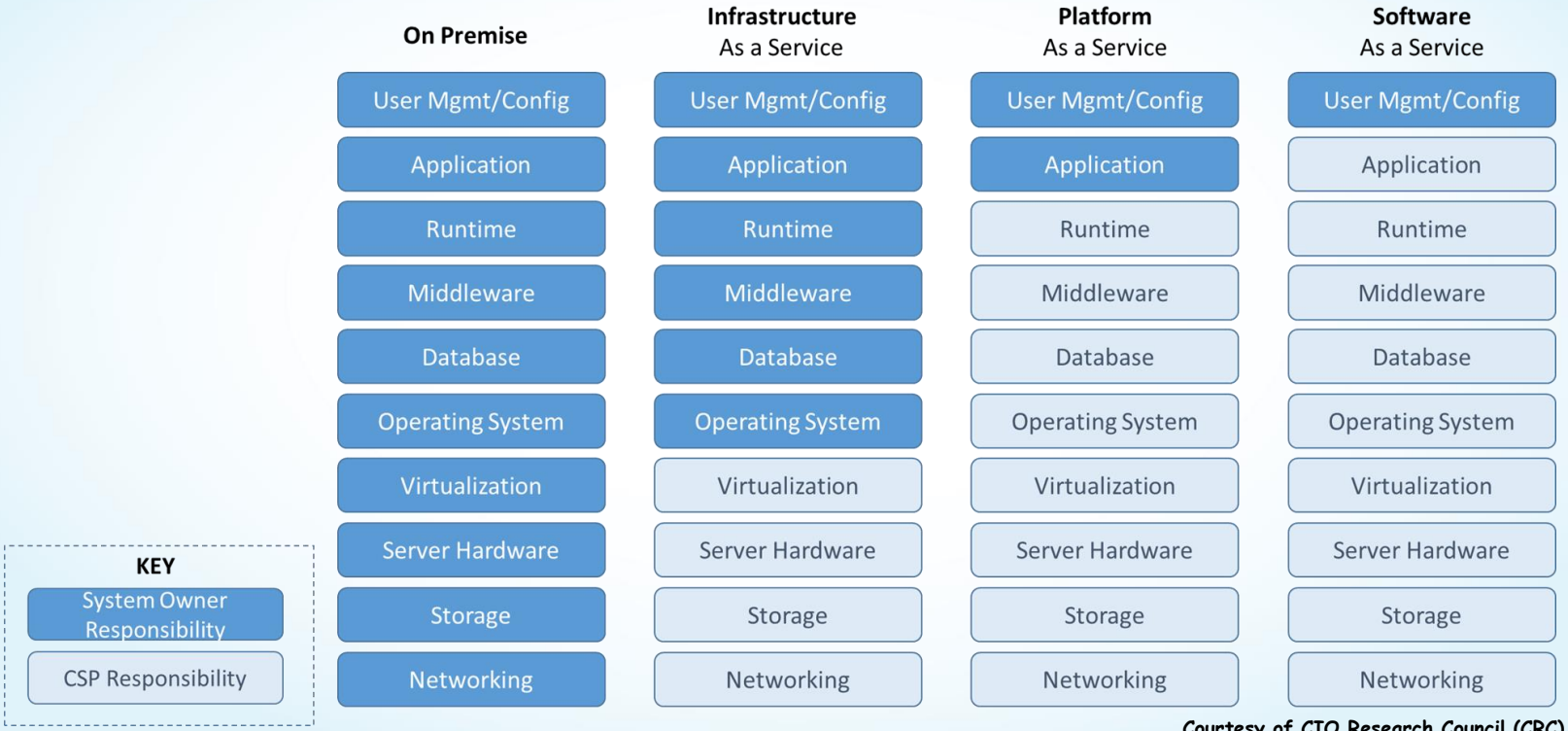
- Options
  - Cloud Service Provider (CSP) – e.g., Amazon, Microsoft, Google providing cloud services such as AWS, Azure, G-Suite
  - Cloud Customer – Mission or System Owner (SO) (e.g., within a Federal Agency) leveraging a cloud service offering

How to identify the boundary of security responsibility?

Security Responsibility Boundary Identification Challenges

- Complex Architecture(s) of Modern Systems
- Confusing concepts related to security control inheritance and common controls
- Lack of clear guidance on how to identify the SO’s security responsibility

Responsibility in Cloud Service Models



Courtesy of CIO Research Council (CRC)

Available Security Guidance (I)

- NIST Risk Management Framework (RMF)
  - SP 800-37
    - 6-Step RMF Security Lifecycle
  - SP 800-53
    - Catalog of Security Controls
    - Security Control Baselines (Low, Moderate, High)
    - **Process for Selection and Specification of Security Controls**

Available Security Guidance (II)

- FedRAMP
  - Guidance for CSPs to obtain authorization
  - Guidance for Agencies
    - Agency Authorization
    - **Reuse of Existing FedRAMP Authorizations**
    - Acquisition of Cloud Services
  - Templates for Authorization
    - **Control Implementation Summary (CIS) Workbook**

Available Security Guidance (III)

- DoD Instruction 8510.01
  - RMF for DoD Information Technology
- DoD CNSI 1253
  - Security Categorization and Control Selection for National Security Systems (NSS)
  - **Table D-2: Potential inheritability of RMF security controls**
- DoD Cloud Computing Security Requirements Guide
  - FedRAMP+ Tailored Baseline
  - Provisional Authorization (PA) from DISA

How to Make the SO's Job Easier?

1. Rethink the Cloud Security Architectural Model
2. Clarify concept of Common Controls
3. Provide a methodology to identify the SO's retained security responsibility

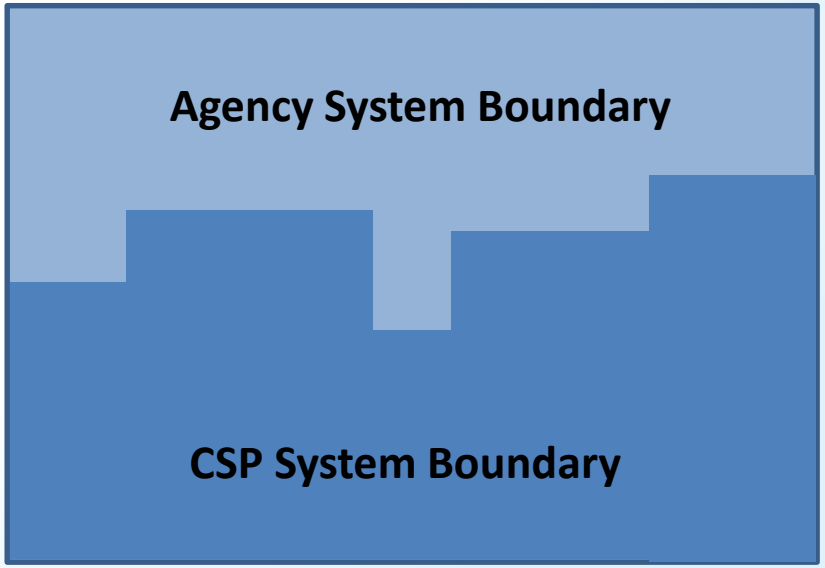
1. Rethinking the Cloud Security Architectural Model

Reality of the Modern Day Cloud-based Information System

- Leverages one or more Cloud Service Providers (CSP)
  - E.g., SaaS built on a IaaS
- May also leverage other organizational information systems
  - Common Control Providers (CCP)
  - General Support Systems (GSS)

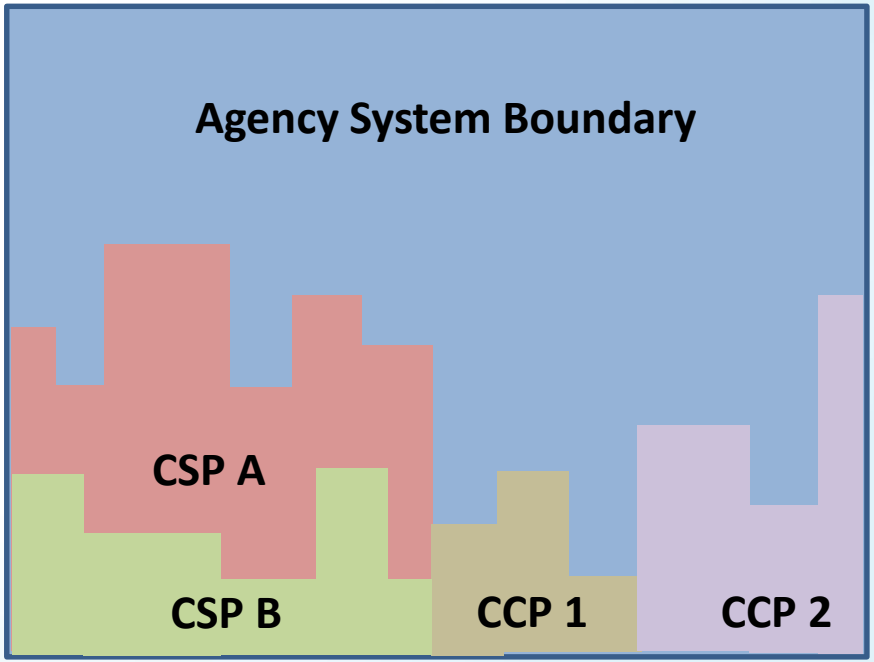
FedRAMP Model for Security Authorization Boundaries

- CSP Boundary gets a lot of attention for FedRAMP Authorization
- Seems to imply that Agency Cloud System can only inherit controls from 1 CSP



New Model for Security Authorization Boundaries

- Agency System can leverage multiple CSPs and Organizational Common Control Providers (CCPs)
- Controls can be inherited from
  - CSPs
  - CCPs



2. Clarifying the Concept of Common Controls

NIST Security Control Designations

- *Common Control* – A security control that is inherited by one or more **organizational** information systems.

- *Hybrid Control* – A security control that is implemented in an information system in part as a common control and in part as a system-specific control.

- *System-Specific Control* – A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

Current Terminology is Confusing!

- A CSP is an external organization
  - Confusing to describe CSP controls as “common” to the Cloud Customer organization!
- Typical “common controls” within an organization include policies & procedures, staff training, acquisition, physical protection
  - Inappropriate to be considered “common” when talking about CSPs.

Proposed New Terminology for Security Control Designations (I)

- Current: *Common Control* – A security control that is inherited by one or more organizational information systems.

- Proposed: *Fully-Inherited Control* – Security control that provides protection to the information system but is fully implemented by another information system. Can be of 2 types:
  - Common Control – A security control inherited from another **organizational** information system.
  - External Control – A security control inherited from an information system implemented by an entity external to the organization.

Proposed New Terminology for Security Control Designations (II)

- Current: *Hybrid Control* – A security control that is implemented in an information system in part as a common control and in part as a system-specific control.

- Proposed: *Partially-Inherited Control* – Security control that is partially implemented by the information system and partially implemented by another information system.

Proposed New Terminology for Security Control Designations (III)

- Current: *System-Specific Control* – A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

- Proposed: *System-Specific Control* – A security control for an information system that has not been designated as a **fully-inherited** security control or the portion of a **partially-inherited** control that is to be implemented within an information system.

3. Methodology to identify the System Owner's retained security responsibility

FedRAMP Control Implementation Summary (CIS) Workbook Template (CSP fills out)

Control ID	Implementation Status					Control Origination						
	In Place	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid	**Configured by Customer**	**Provided by Customer**	**Shared Responsibility**	Inherited from Pre-Existing Authorization
AC-01												
AC-02												

- Configured by Customer – customer applies a configuration
- Provided by Customer – customer provides additional HW or SW
- Shared Responsibility
  - Independent Shared – both parties have to implement control independently
  - Dependent Shared – each party implements parts of control

Relevant RMF Process Steps …

- RMF Step 1: Categorize
- RMF Step 2: Select
  - Control Selection
  - Control Tailoring
  - **Control Allocation**
  - Control Documentation
  - …

Proposed Control Allocation Methodology (I)

- Identify Controls Inherited from CCPs
  - Identify CCPs available within Organization
  - Review Security Controls implemented by CCPs
  - Designate appropriate controls as
    - Fully-Inherited
    - Partially-Inherited

Proposed Control Allocation Methodology (II)

- Identify Controls Inherited from CSP
  - Review CIS Worksheet from CSP FedRAMP package
  - Consider Full Inheritance of CSP controls not marked as:
    - Configured by Customer
    - Provided by Customer
    - Shared Responsibility (Independent Shared)
  - Consider Partial Inheritance of CSP controls marked as:
    - Shared Responsibility (Dependent Shared)
    - Document which parts remain to be implemented

Proposed Control Allocation Methodology (III)

- Identify as System-Specific all of the controls not yet marked as:
  - Fully-Inherited
  - Partially-Inherited
- Determine extent of SO responsibility for partially-inherited controls

The system-specific controls are the SO's retained security responsibility!

Summary

1. Cloud-based Information Systems are at risk if the SO's retained security responsibility is underestimated
2. Controls can be inherited from CCPs as well as CSPs
3. Apply new terminology of Fully-Inherited and Partially-Inherited Controls to allocate controls
4. Utilize the CIS Worksheet from the CSP's FedRAMP SSP
5. Apply step-by-step process to delineate the SO's retained security responsibility
6. *Better definition of SO's security responsibility results in lower risk!*

TELL US WHAT YOU THINK!

Evaluate this session right in the GRC Conference App!

CONTACT INFORMATION

Dr. Sarbari Gupta, CISSP, CISA
President & CEO
Electrosoft
Email: sarbari@electrosoft-inc.com
Phone: 703-437-9451 ext. 12
LinkedIn: http://www.linkedin.com/profile/view?id=8759633