Shared Responsibility is NOT Shared Risk!

Managing Risk in a Shared Responsibility Environment

November 11, 2019

icebergnetworks.com

Who am I?

MBA, CISSP

30+ year history in security, technology, and management consulting, including

- Technology for Nuclear and Biomedical research
- Information technology / Information security
- Telecom software
- Managed Security Services
- Mergers, acquisitions, acquisition integration

Co-founder of Iceberg Networks – Solely focused on GRC program consulting and implementation

Super-power: I can peel labels off things (even those paper labels that fall apart)

RSA Iceberg

What am I here to talk about?

Managing risk in a shared responsibility environment

The differences between issue, risk, vulnerability, and uncertainty

The complexities of assurance activities

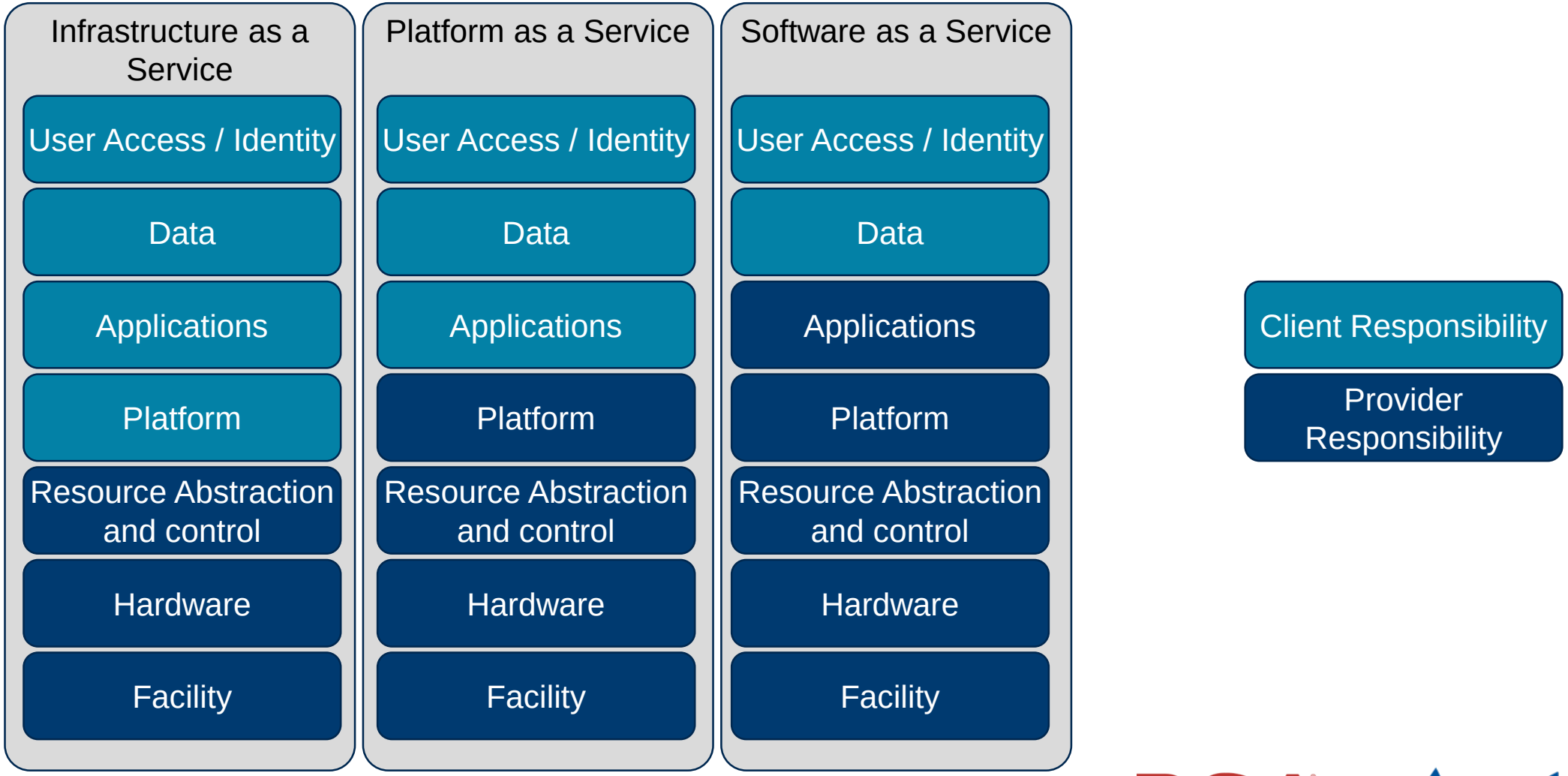
Models for managing the complexity

My CRC Digital Transformation Dream

Problem #1 – Shared Responsibilities

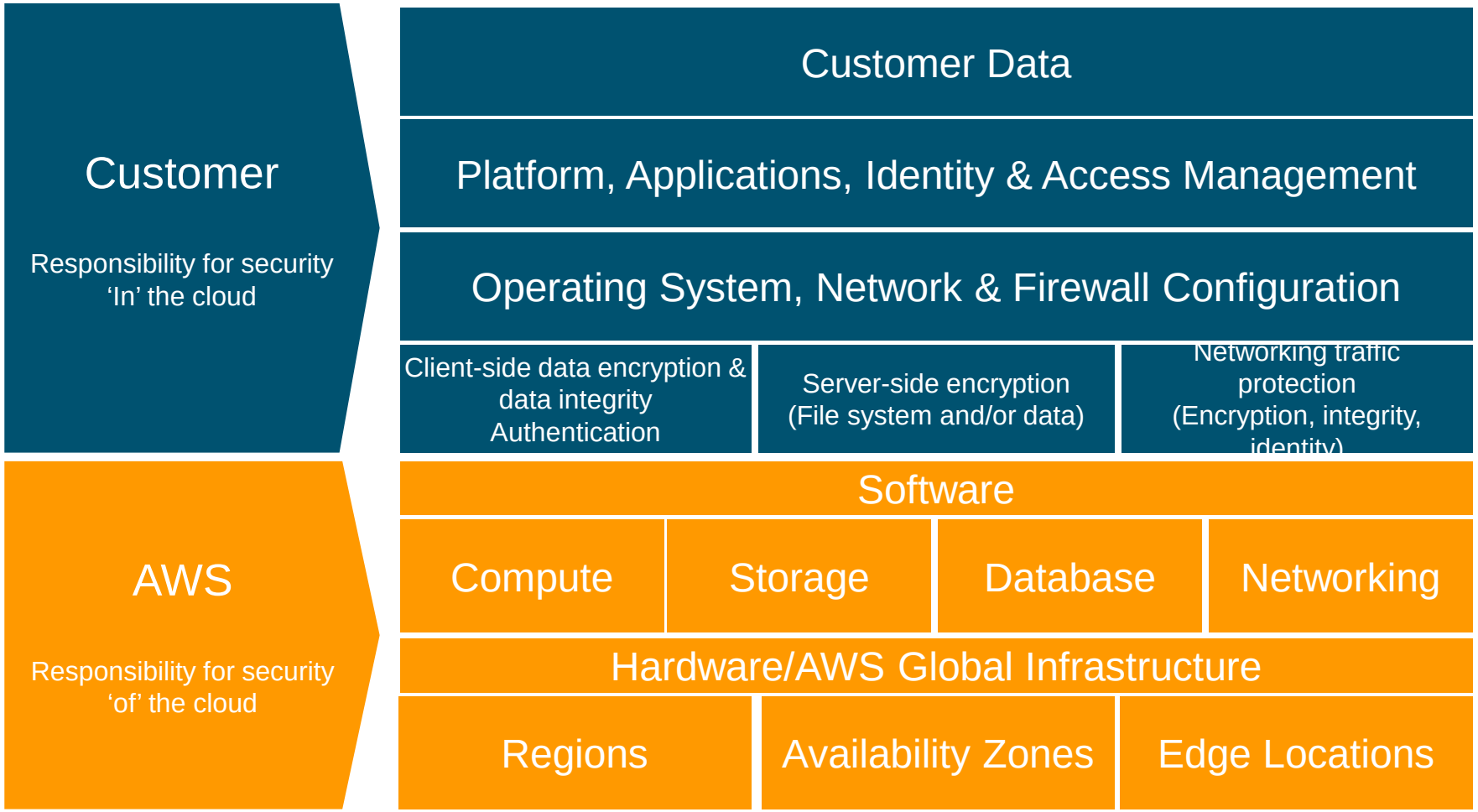
Tip: You can share responsibility, but you can’t share accountability.

Shared Responsibility Models



Source: Canada.ca

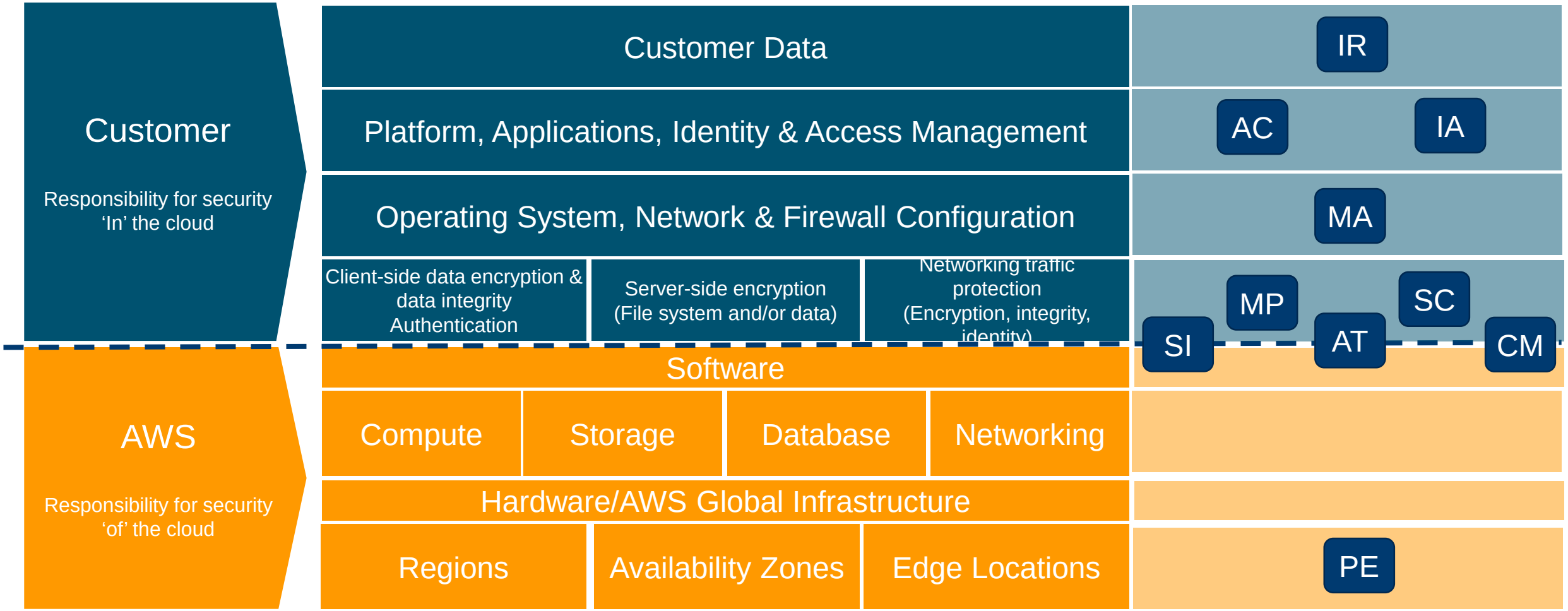
Shared Responsibility Model (AWS)



Source: https://aws.amazon.com/compliance/shared-responsibility-model/

RSA Iceberg

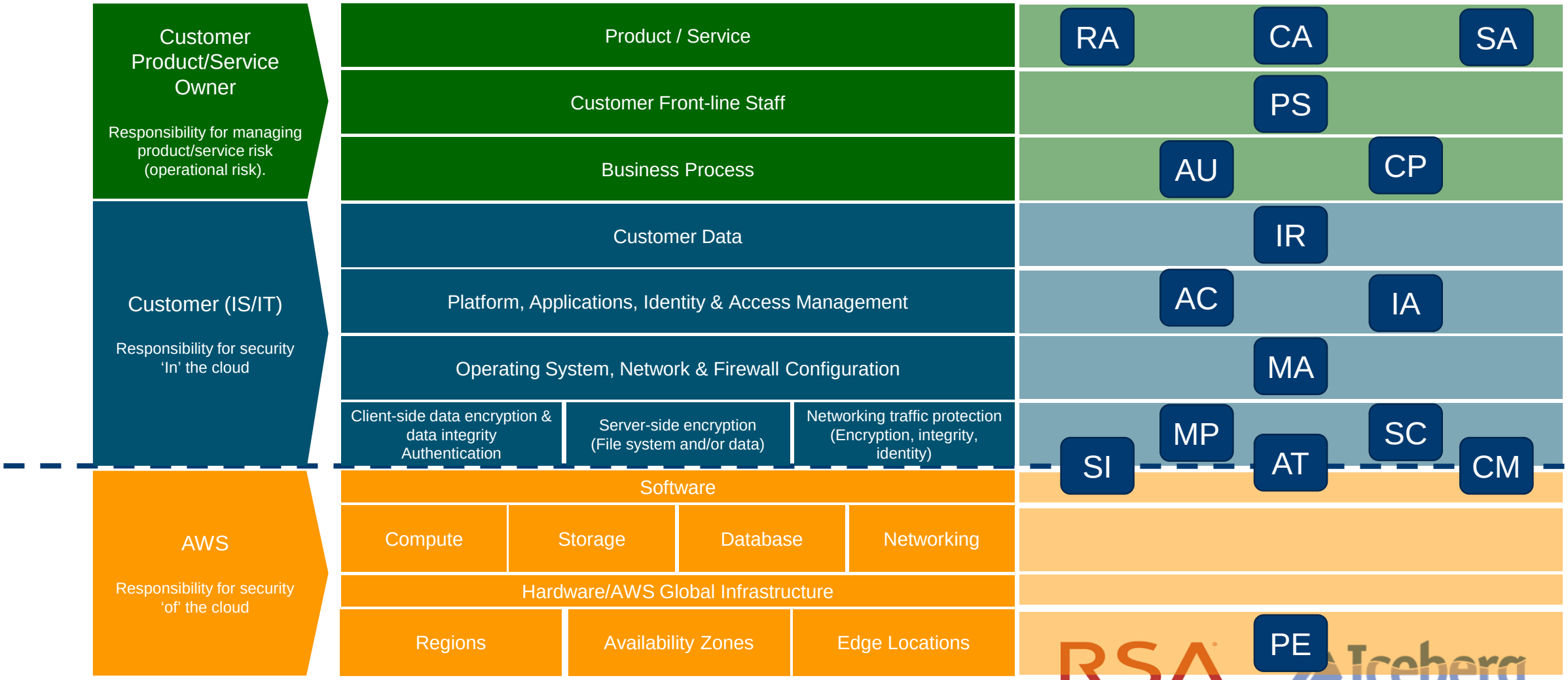
Responsibility = Controls



Derived from: https://aws.amazon.com/compliance/shared-responsibility-model/

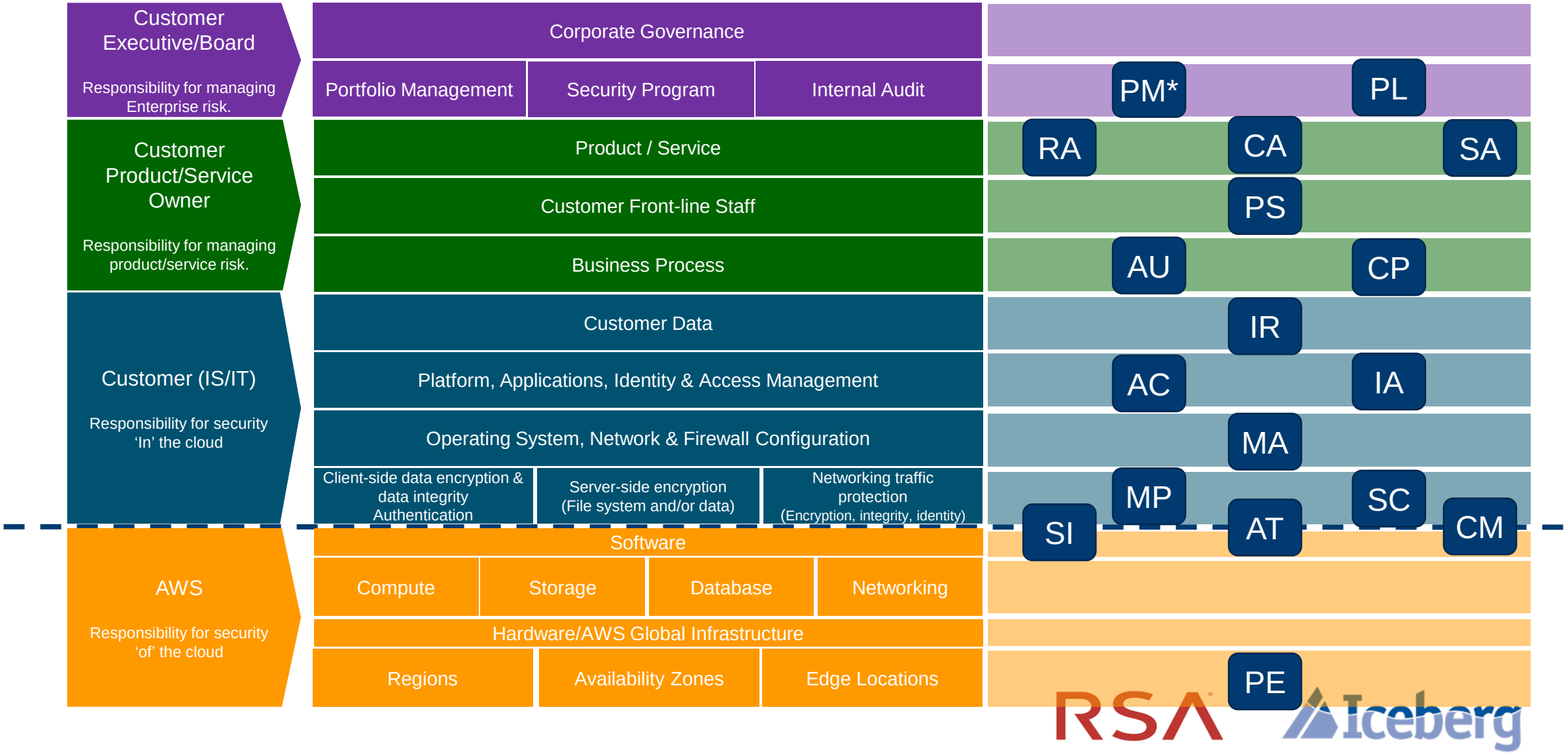
RSA Iceberg

Shared Responsibility Model - Expanded



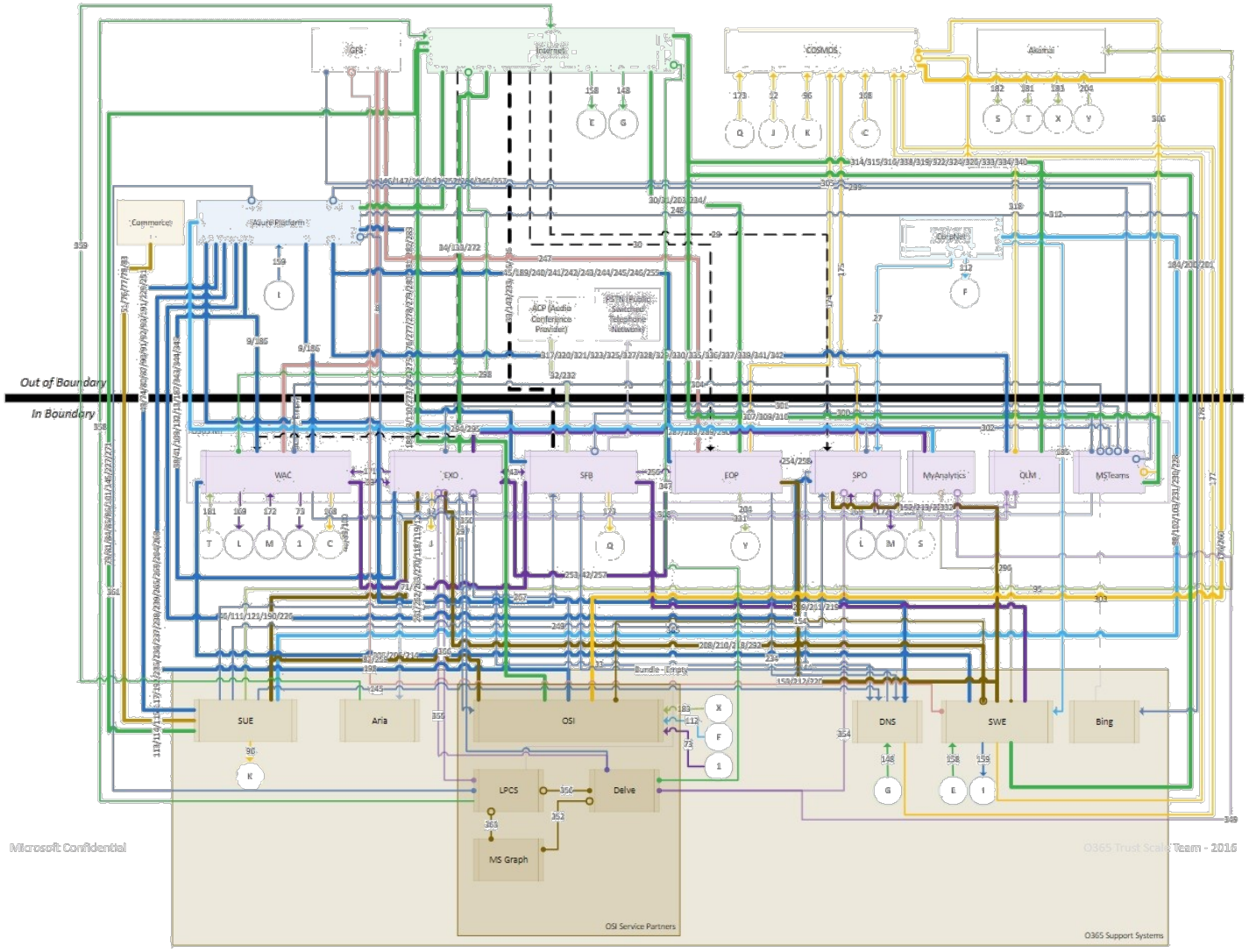
Derived from: https://aws.amazon.com/compliance/shared-responsibility-model/

Shared Responsibility Model – Expanded Again



RSA Iceberg

It’s Never That Simple

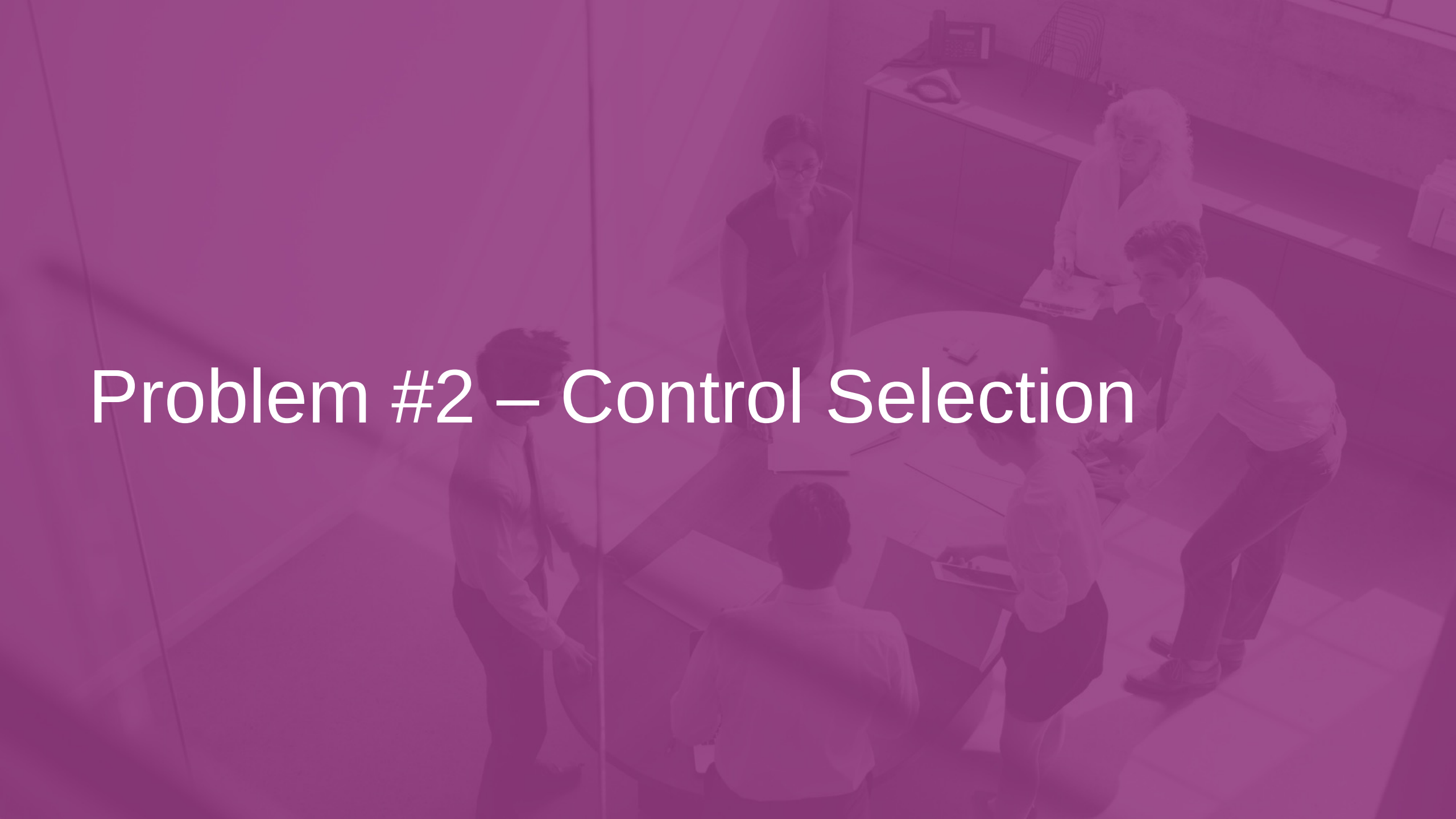


Authorization Boundary Diagram

Source:
FedRAMP System Security Plan (SSP)
for
Office 365 MultiTenant (MT)

Microsoft Corporation

RSA Iceberg



Problem #2 – Control Selection

The Control Framework Problem

Source	Control Categories (Families)	Controls	Provider Controls
NIST SP800-53 and FedRAMP (Moderate Baseline)	17	325	Self Selection
SOC 2 (System and Organization Controls) - AICPA Trust Services Criteria	13	69	69
SIG (Standardized Information Gathering)	16	1506	1506
GC PBMM Cloud Profile	17	469	335
PCI DSS	13	246	246
Privacy (eg Privacy Act, FIPPA, HIPPA, GDPR)	Various		
Industry-Specific Compliance requirements (eg NERC CIP, OSFI Guidelines)	Various		

RSA Iceberg

Problem #3 – Risk Terminology

Risk Vocabulary

Communications Gaps

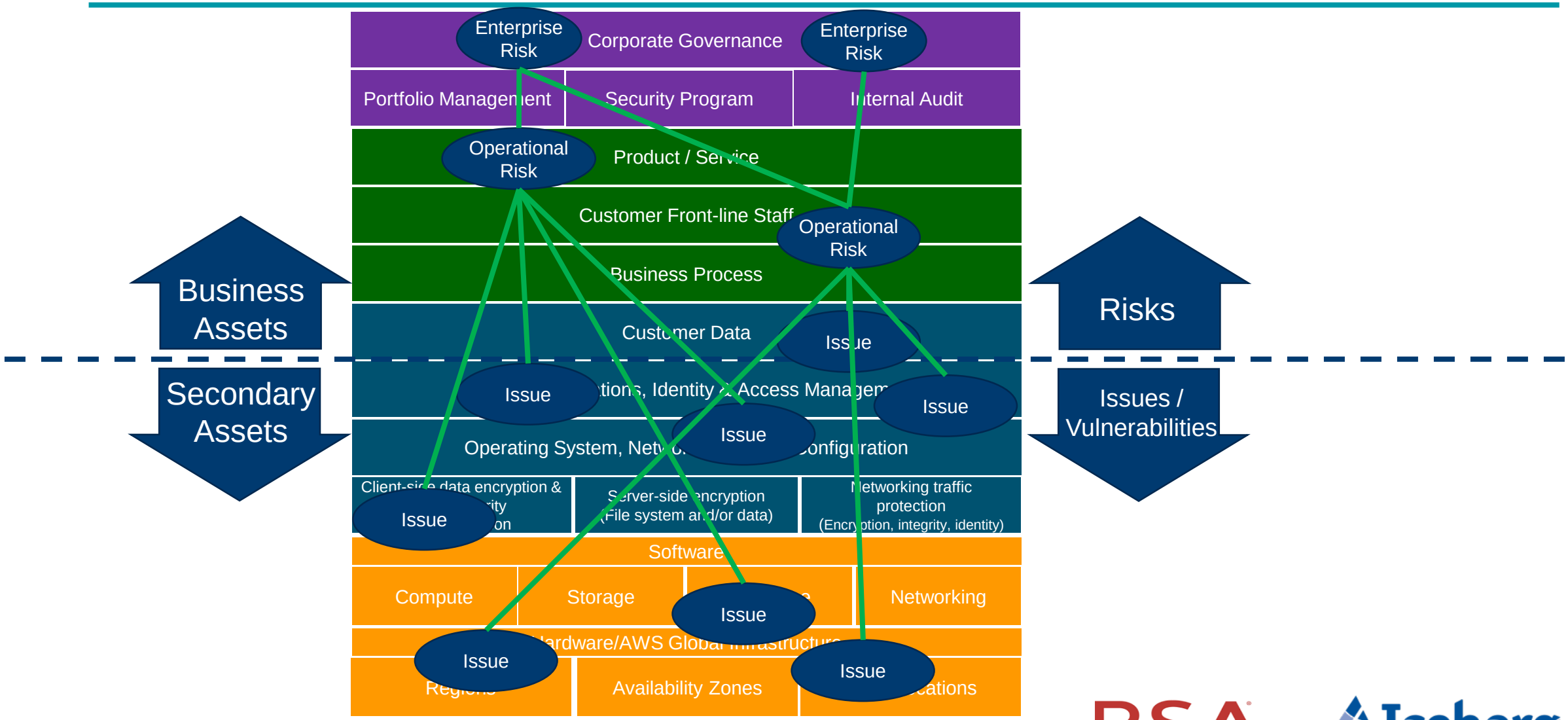
Elements of Risk

$$Risk = f(A_{val}, T, V)$$

Source: Harmonized TRA Methodology

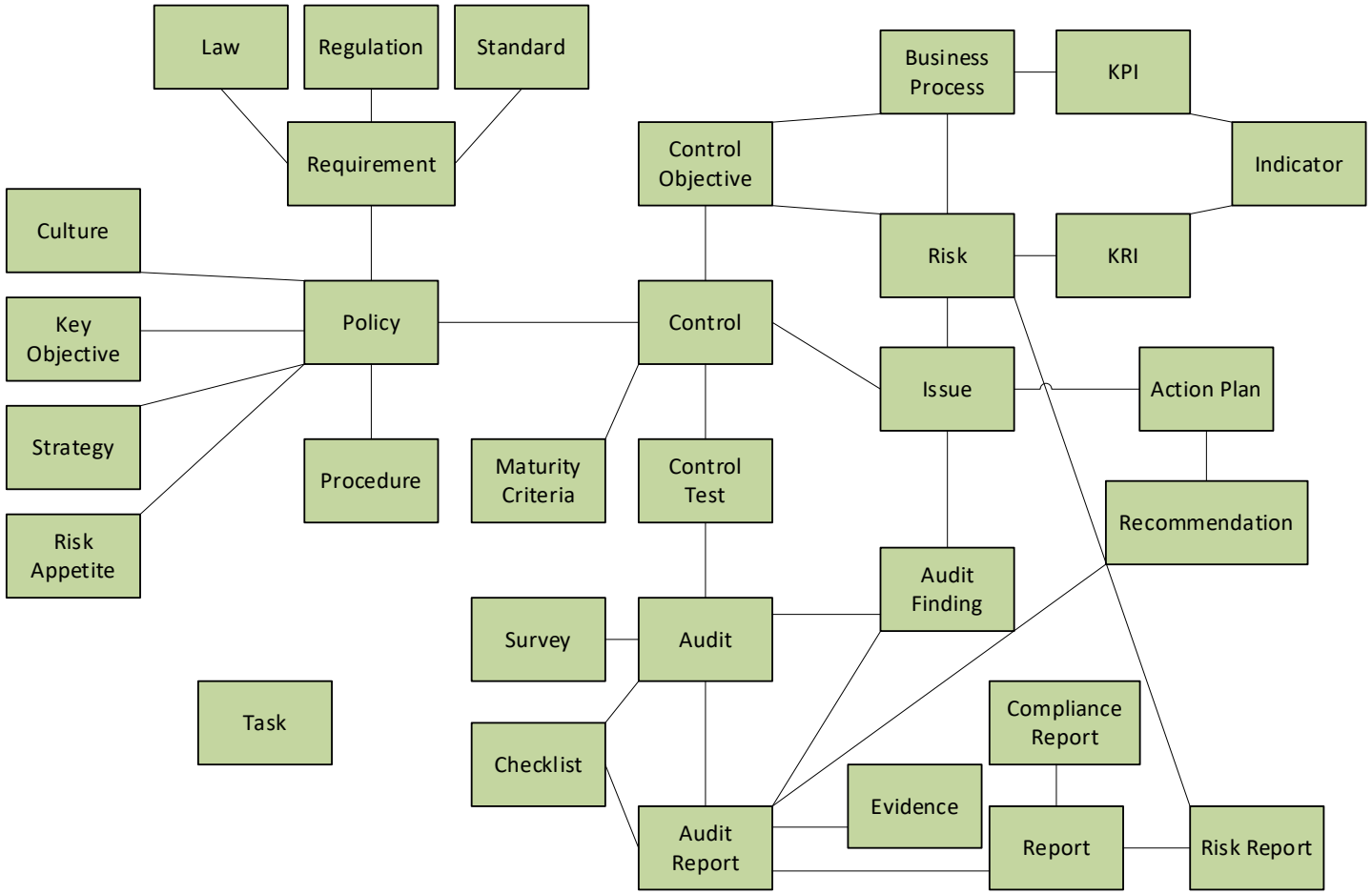
$A_{val} = Asset\ Value$
$T = Threat$
$V = Vulnerability$

Risk vs Issue



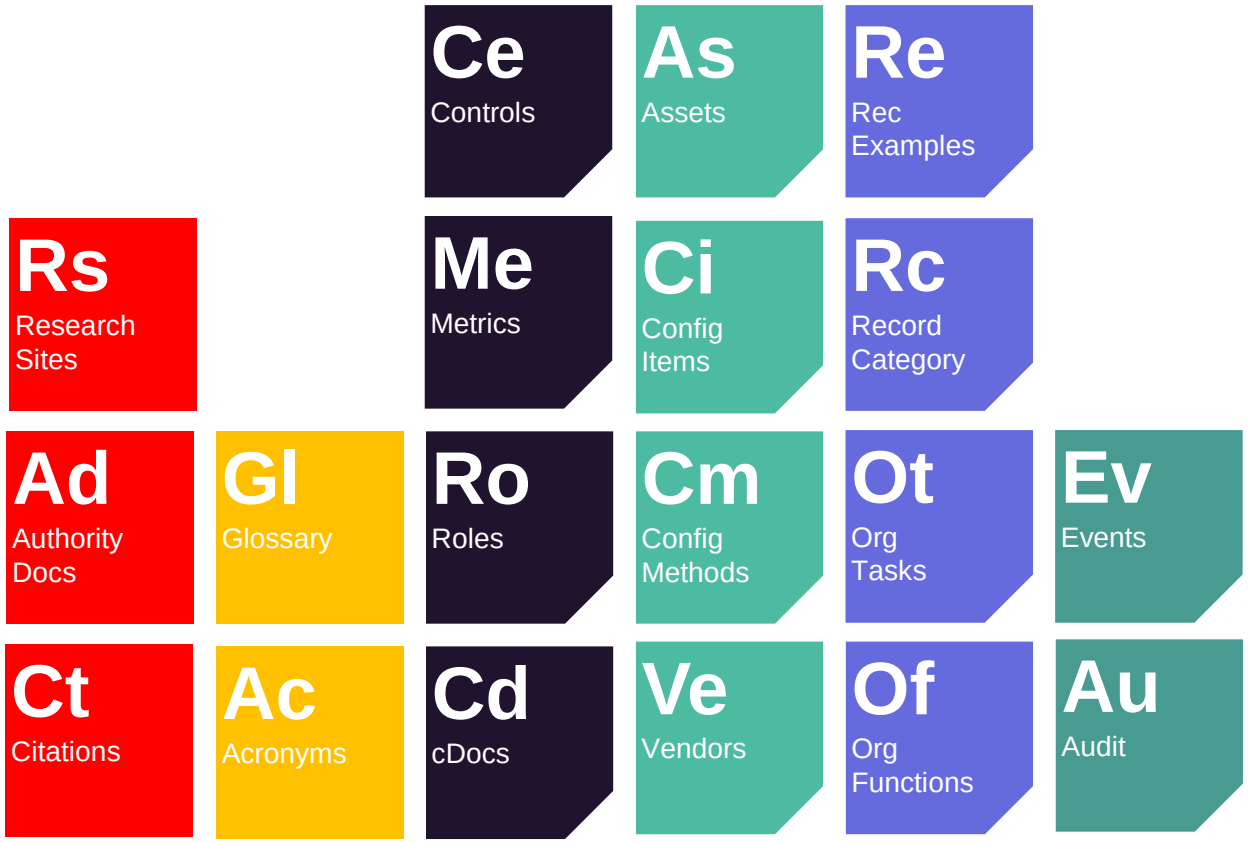
Solution: GRC Systems

GRC Reference Model



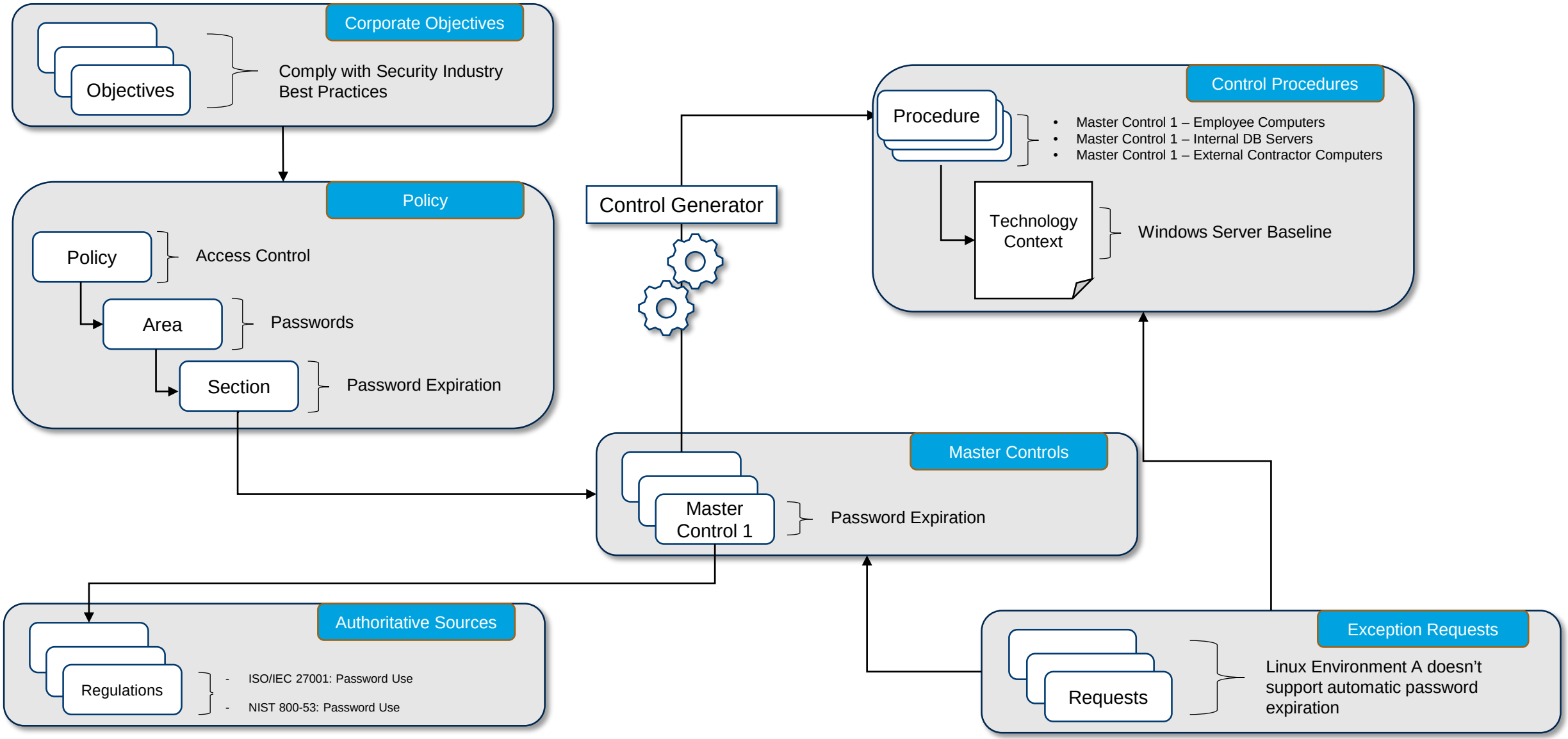
Source: *Towards a Reference Model for Integrated Governance, Risk and Compliance*. Vicente, Racz, Mira da Silva

UCF Reference Model

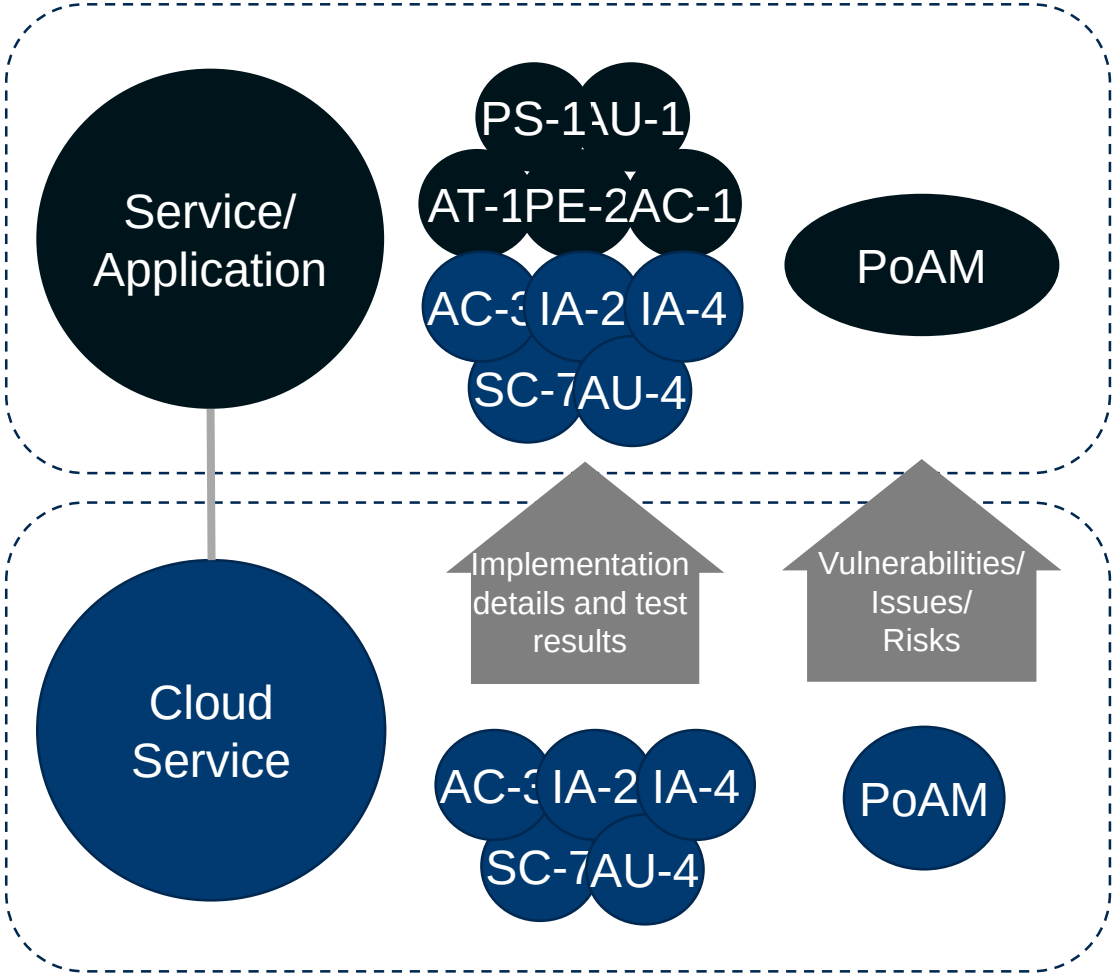


Source: Unified Compliance Framework

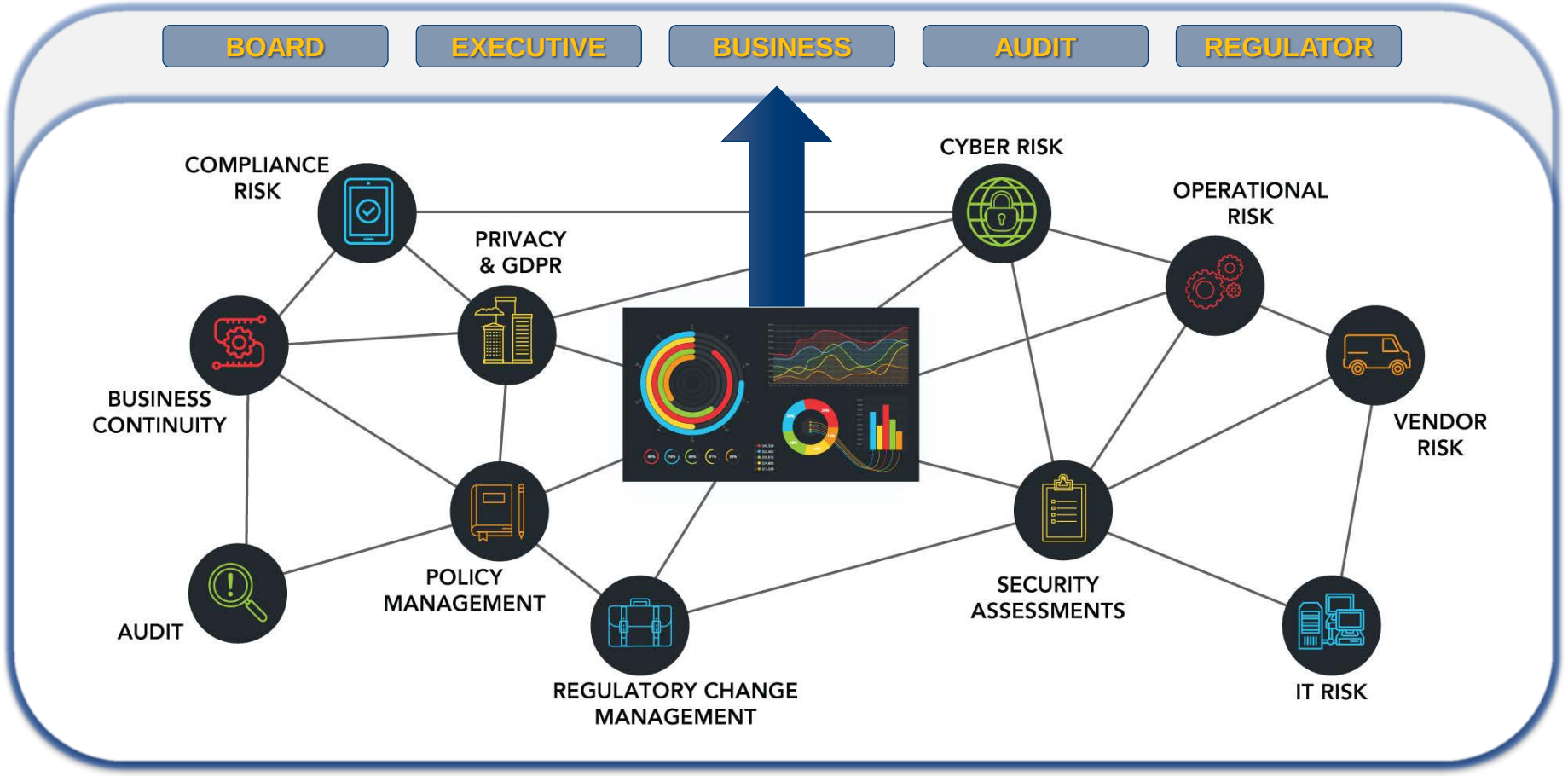
Controls Management Structure Implementation



GRC Federation



Integrated Risk Management Functions



"**Confident business decision making** requires compiling and analyzing risk data from **a complex web of interrelated areas and disciplines.**"

RSA Iceberg

Summary

- Security architecture can be a daunting task, but a systematic approach to security boundary definition will help
- Control allocation can result in 1000’s of interrelated data points that need to be managed
- Relationships between assets, threats, risks and controls are not linear and require tools to clearly measure, manage and communicate risk
- Poor communications can result in dramatic misunderstanding of risk

RSA Iceberg

Thank you.

icebergnetworks.com

References

- https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html
- https://aws.amazon.com/compliance/shared-responsibility-model
- https://www.microsoft.com/en-us/trustcenter/Compliance/fedramp
- https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance
- https://www.unifiedcompliance.com/
- https://fenix.tecnico.ulisboa.pt/downloadFile/395142791115/resumo.pdf

RSA Iceberg