



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)



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 SRS Digital Transformation Dream

Problem #1 – Shared Responsibilities

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

Shared Responsibility Models



Source: Canada.ca



Provider Responsibility

Shared Responsibility Model (AWS)

	Customer Data Platform, Applications, Identity & Access Management						
Customer							
Responsibility for security 'In' the cloud	Operating System, Network & Firewall Configuration						
	Client-side data encry data integrity Authentication	ption &	Server-side encryption (File system and/or data)		Networking traffic protection (Encryption, integrity, identity)		
	Software						
AWS	Compute	Storage		Database		Networking	
Responsibility for security	Hardware/AWS Global Infrastructure					ure	
Regions			Availabil	ity Zones		Edge Locations	

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

RSA AIceberg

Responsibility = Controls

Ę



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

RSA Alceberg

Shared Responsibility Model - Expanded

Customer Product/Service		Product	/ Service			RA CA SA			
Owner Responsibility for managing	Customer Front-line Staff					PS			
product/service risk (operational risk).	Business Process					A	AU	СР	
	Customer Data					IR			
Customer (IS/IT)	Platform, Applications, Identity & Access Management				A	AC	IA		
Responsibility for security 'In' the cloud	Operating System, Network & Firewall Configuration				МА				
	Client-side data encryption & data integrity Authentication	Server-side encryption (File system and/or data)		Netwoi (En	king traffic protection cryption, integrity, identity)			SC	
	Software) –	
AWS	Compute	Storage	Databas	e	Networking				
Responsibility for security	Hardware/AWS Global Infrastructure								
	Regions	Availability Zones		Edge Locations		RS	PE	Tcehero	1
								TCCDCIG	

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

Shared Responsibility Model – Expanded Again

Customer Executive/Board									
Responsibility for managing Enterprise risk.	Portfolio Management	Security Progr	am	Internal Audit	PM*			PL	
Customer Broduct/Sonvice		RA		CA		SA			
Owner				PS					
Responsibility for managing product/service risk.	Business Process					AU		CP	
		Customer Data					IR		
Customer (IS/IT)	Platform, A	oplications, Identity 8	Access M	lanagement	AC IA				
Responsibility for security 'In' the cloud	Operating	Operating System, Network & Firewall Configuration					MA		
	Client-side data encryption data integrity Authentication	& Server-side encry (File system and/o	ver-side encryption system and/or data) Networking traffic protection (Encryption, integrity, identity)			MP		SC	
		SI		AI					
AWS	Compute	Storage	Database	Networking					
Responsibility for security	На								
	Regions	Availability Zones		Edge Locations		C A ¹	PE	T 1	
					R	S/		ice b	pera

J

It's Never That Simple



Authorization Boundary Diagram

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

RSA AIceberg

Microsoft Corporation

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
PCIDSS	13	246	246
Privacy (eg Privacy Act, FIPPA, HIPPA, GDPR)		Various	
Industry-Specific Compliance requirements (eg NERC CIP, OSFI Guidelines)		Various	
13 icebergnetworks.com		RSA	A Iceberg

Problem #3 – Risk Terminology

Risk Vocabulary



icebergnetworks.com 15

Communications Gaps

What we say to dogs



what they hear

Sea .



Elements of Risk

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

Source: Harmonized TRA Methodology

 $A_{val} = Asset Value$ T = ThreatV = 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

RSA AIceberg

UCF Reference Model



Source: Unified Compliance Framework

RSA AIceberg

21 icebergnetworks.com

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 Alceberg

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







Thank you.

icebergnetworks.com

References

- <u>https://www.canada.ca/en/government/system/digital-government/modernemerging-technologies/cloud-services/government-canada-security-controlprofile-cloud-based-it-services.html</u>
- <u>https://aws.amazon.com/compliance/shared-responsibility-model</u>
- <u>https://www.microsoft.com/en-us/trustcenter/Compliance/fedramp</u>
- <u>https://en.wikipedia.org/wiki/Governance, risk_management, and complian</u>
 <u>ce</u>
- https://www.unifiedcompliance.com/
- https://fenix.tecnico.ulisboa.pt/downloadFile/395142791115/resumo.pdf

