

W W W . C L O U D C O P . C O M

Cloud Cop Introduction

Our Mission

Cloud Cop enables
Cloud Governance
in a simple and
affordable way

Why

Proactive control of cost and security with **insight**

Ensure that technology complies with the company's requirements

Lowers the risk

Lowers the cost

How

Simplify Cloud Governance

Continuously monitor **cost** and **Security**

Report and act on deviations

Being an independent auditor

Microsoft Cloud Adoption Framework



Microsoft Cloud Adoption Framework

- Define Corporate Policy

Govern

Define Corporate Policy

Business Risks ·····



Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality



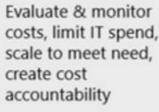
Convert Risk decisions into policy statements to establish cloud adoption boundaries.



Establish processes to monitor violations and adherence to corporate policies.

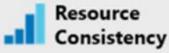
Microsoft Cloud Adoption Framework - Five Disciplines of Cloud Governance

Cost Management





Ensure compliance with IT Security requirements by applying a security baseline to all adoption efforts



Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability

Five Disciplines of Cloud Governance



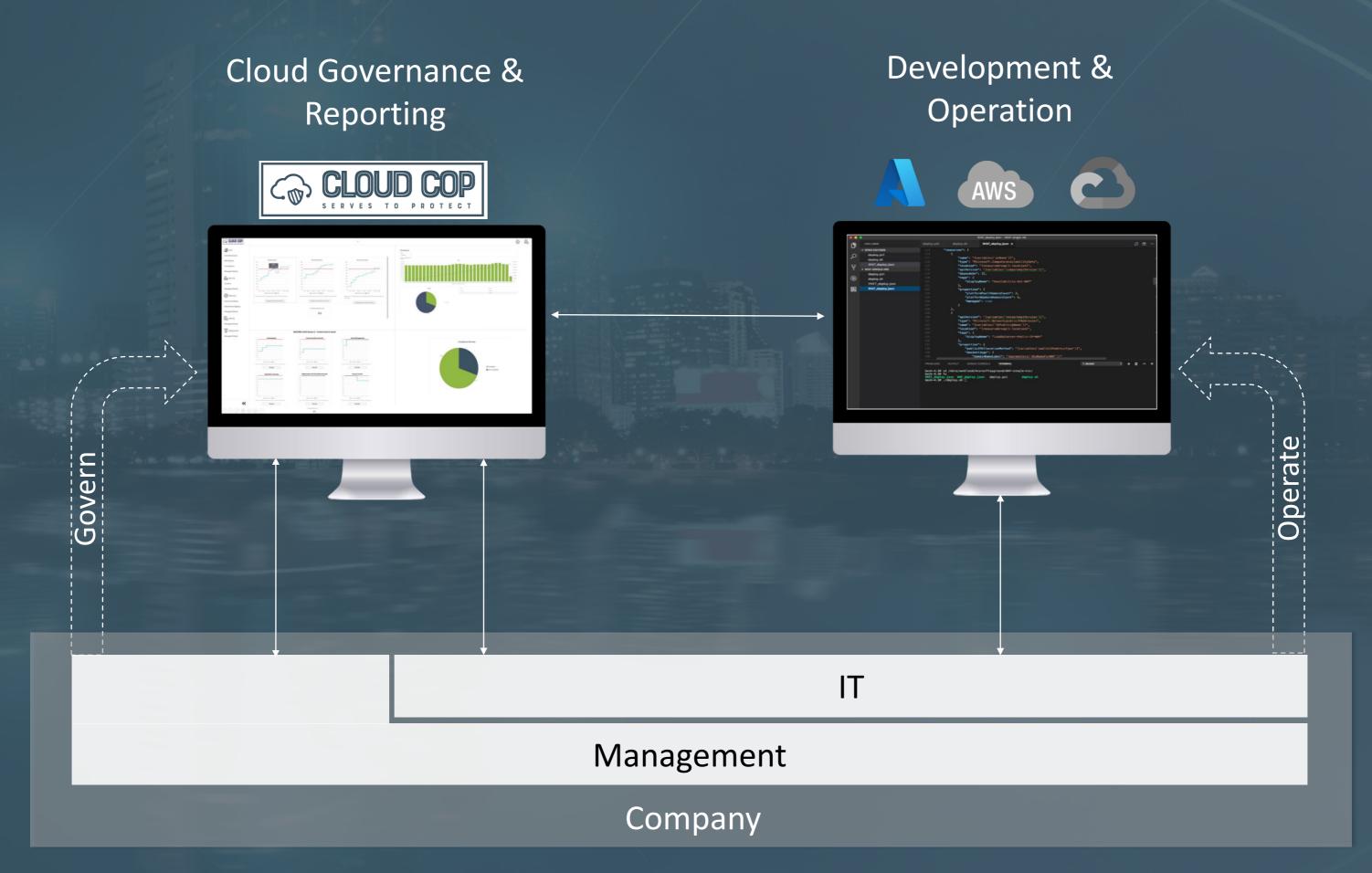
Identity Baseline

Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments



Accelerate deployment through centralization, consistency, and standardization across deployment templates

Closing the gap between management and IT



Security Frameworks - continuous reporting

ISO 27001:2013 - Azure Report - 2023

			Development	YTD	End last Year	January	February	March	April	May	June	July	August	September	October	November	December
73 %	Automatic	Organization of Information Security	n		100 %												
	Automatic	Asset Management	•		100 %												
	Automatic	Access Control	2		80 %												
	Automatic	Cryptography	20		69 %												
	Automatic	Operations Security	2		42 %												
	Automatic	Communications Security	20		O 50 %												
0 %	Manual	Context of the organization	₩		0 %												
	Manual	Leadership	₩		0 %												
	Manual	Planning	₩		0 %												
	Manual	Support	₩		0 %												
	Manual	Operation	₩		0 %												
	Manual	Performance Evaluation	₩		0 %												
	Manual	Improvement	₩		0 %												
	Manual	Information Security Policies	₩		0 %												
	Manual	Human Resources Security	₩		0 %												
	Manual	Physical And Environmental Security	₩		0 %												
	Manual	System Acquisition, Development And Maintenance	₩		0 %												
	Manual	Supplier Relationships	₩		0 %												
	Manual	Information Security Incident Management	₩		0 %												
	Manual	Information Security Aspects Of Business Continuity Management	₩		0 %												
	Manual	Compliance	₩		0 %												



Active Customer All





















SOC 2 Type 2

ISO 27001:2013

NIST SP 800-53 Rev. 5

FedRAMP High

HITRUST/HIPAA

PCI v3.2.1:2018

Azure Security Benchm...

Audit Public Network ...

(i) ISO 27001:2013

The International Organization for Standardization (ISO) 27001 standard provides requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). These policies address a subset of ISO 27001:2013 controls. Additional policies will be added in upcoming releases. For more information, visit https://aka.ms/iso27001-init

		View Mode Company	✓ Show all categories
Category	State		
Customer 1 ✓			
Customer 2			
Customer 3	6		
Customer 4			
Customer 5 🗸			
Customer 6			
Customer 7			
Customer 8			
Customer 9 (!)			
Customer 10 🗸			
Customer 11			
Customer 12 ✓			
Customer 13 ✓			
Customer 14 🗸			
Customer 15 🗸			
Customer 16 🗸	6		
Customer 17 🗸			



