



## Zero to Hero: Secure IaC with Bicep

Elkhan Yusubov

 03 May 2023

 17:30 (UTC)



[www.cloudlunchlearn.com](https://cloudlunchlearn.com)

*In collaboration with*



Microsoft

<https://cloudlunchlearn.com>

<https://theCloudMarathoner.com>





**Elkhan Yusubov**

Speaker | Author | Influencer  
Cloud Architect | Founder



Elkhan is a Cloud Architect Manager, Microsoft Azure MVP and 15+ MCT with experience in cloud solutions, enterprise healthcare systems and healthcare data, and API standards (HL7 FHIR, EDI X12).

He is an active Microsoft Tech Community Contributor, Cloud Lunch and Learn Speaker and Co-Organizer, and LinkedIn instructor with interests in Architecture, DevOps & Security.

He is a frequent speaker at tech meetups and has volunteered for Give Camps, Azure Data Fest, SQL Saturdays and Microsoft community events, like this one.

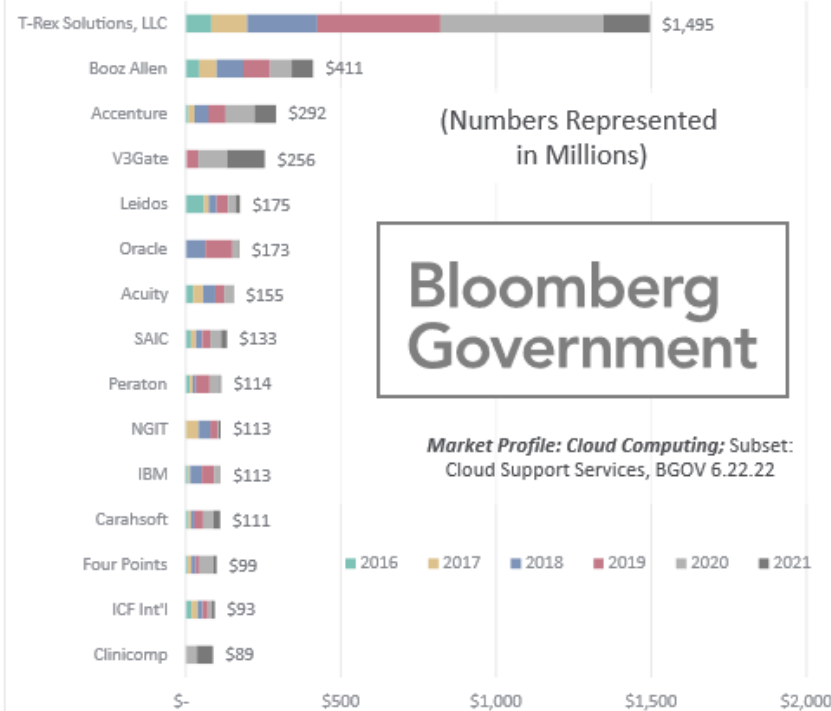
Check out the blog posts at Cloud Marathoner site below.

<https://theCloudMarathoner.com>   

# What we do; where we do it; how it relates



## Top Cloud Support Services Vendors



## Company Info

- **Established:** 1999
- **Legal Structure:** LLC
- **Headquarters:** Greenbelt, MD
- **8(a)/HUBZone & SDVOSB Joint Ventures**
- **CMMI-DEV & SVC Level 3 v2.0**
- **ISO 9001; ISO27001; ISO20000**

### Prime Vehicles/BPAs:

- GSA MAS HACS SIN
- GSA MAS Cloud SIN
- GSA MAS IT Svcs SIN
- COBRA OTA
- CIO-SP3 Small Business
- STARS III via MPJV
- GSA MAS HACS SB & Cloud SIN SB via MPJV

Silver  
**Microsoft Partner**

Silver Datacenter  
Silver Data Analytics  
Silver Data Platform  
Silver App Dev  
Silver App Integration

aws partner network

Advanced  
**Consulting Partner**

Government Competency  
Public Sector Partner



T-Rex has donated over \$3.5M in support of underserved youth, veterans, and local organizations.



# T-Rex's 2020 Census Technical Integration (TI) Program

Census Bureau is one of the first govt agencies to host and protect their mission-critical public-facing applications in the cloud.

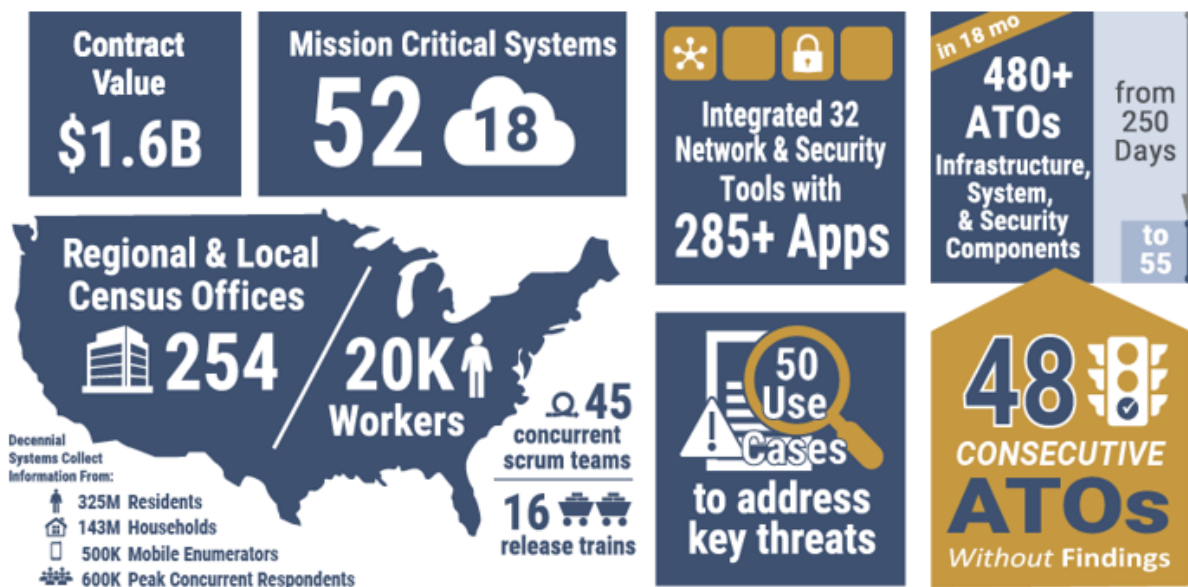
Mission Innovations:

- Improve public access through internet
- Enhance data usage to reduce work
- Boost workforce productivity with mobile computing



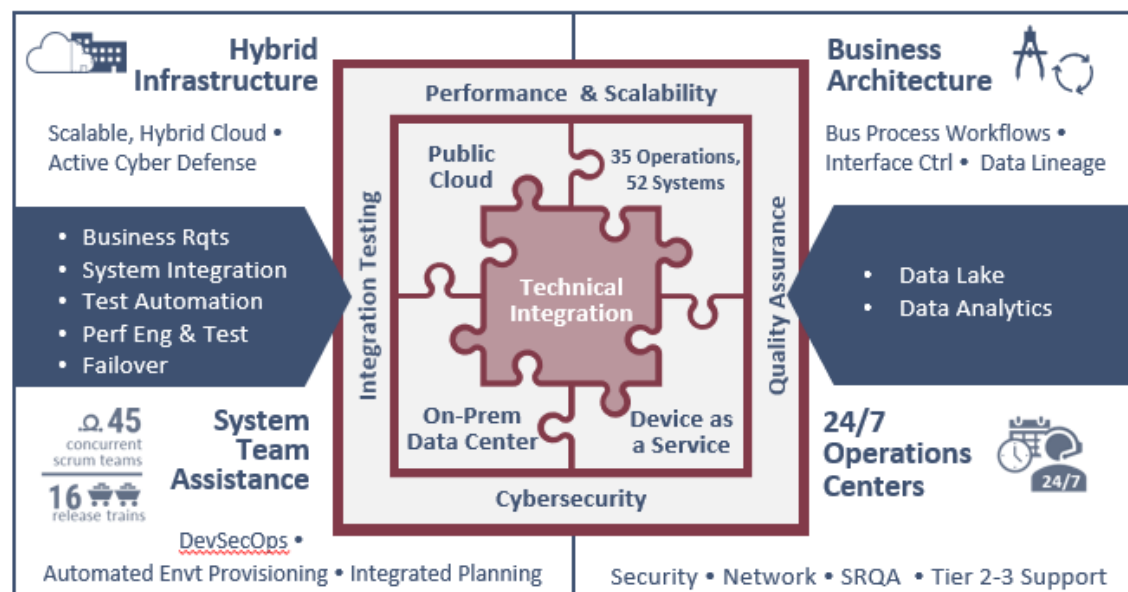
The 2020 Census Technical Integrator (TI) program is one of the largest, most visible government IT transformation programs in size, scale, complexity and scope.

## Size, Scale & Complexity



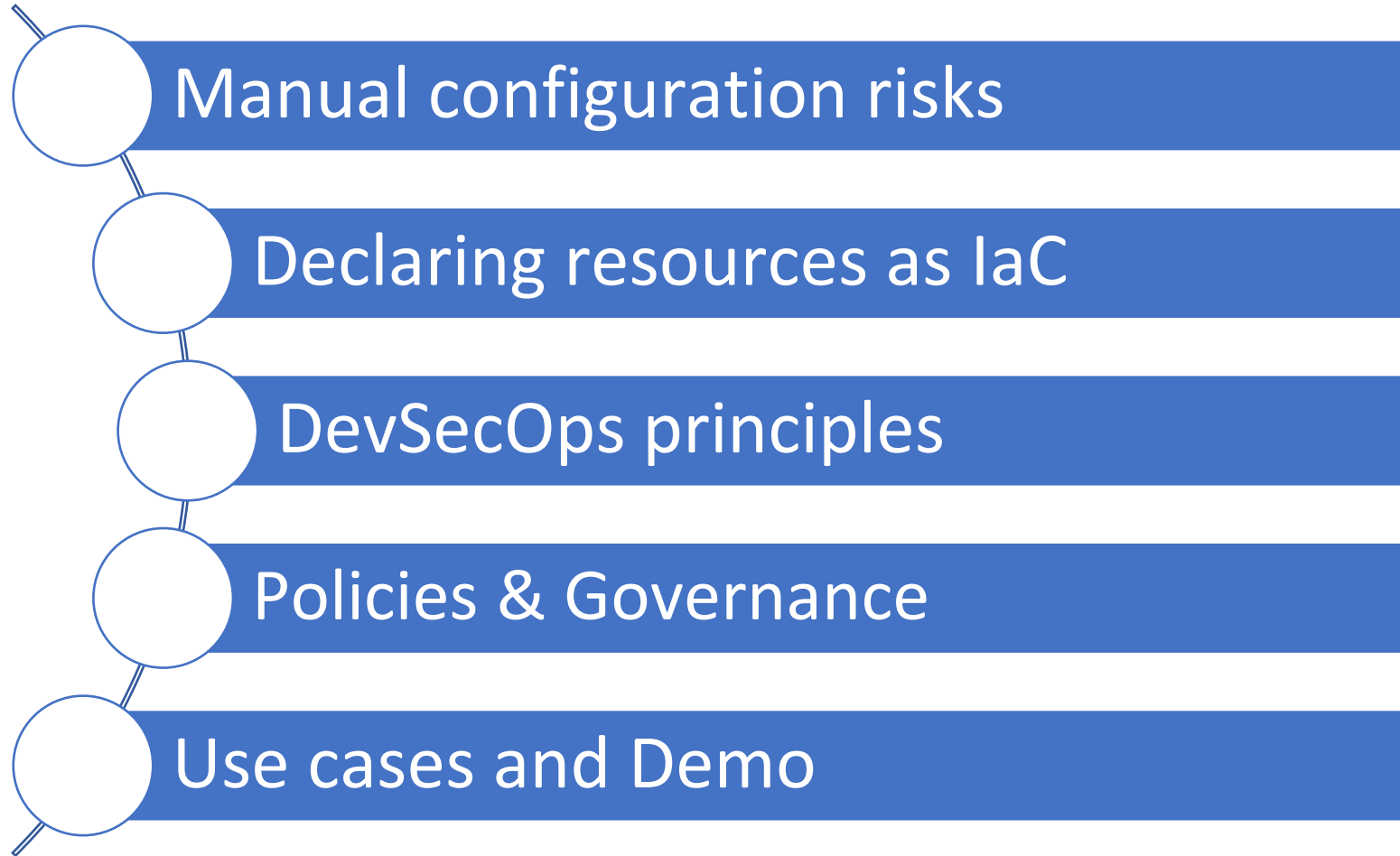
11/7/2020

## Scope



IT Modernization encompassing Cloud, Cyber, Data Analytics, & App Development positioning USCB for the future

# What we will cover





# Manual configuration risks

- Inconsistent Configuration
- Security Risks
- Vendor Lock-in
- Cost Overruns
- Lack of Automation



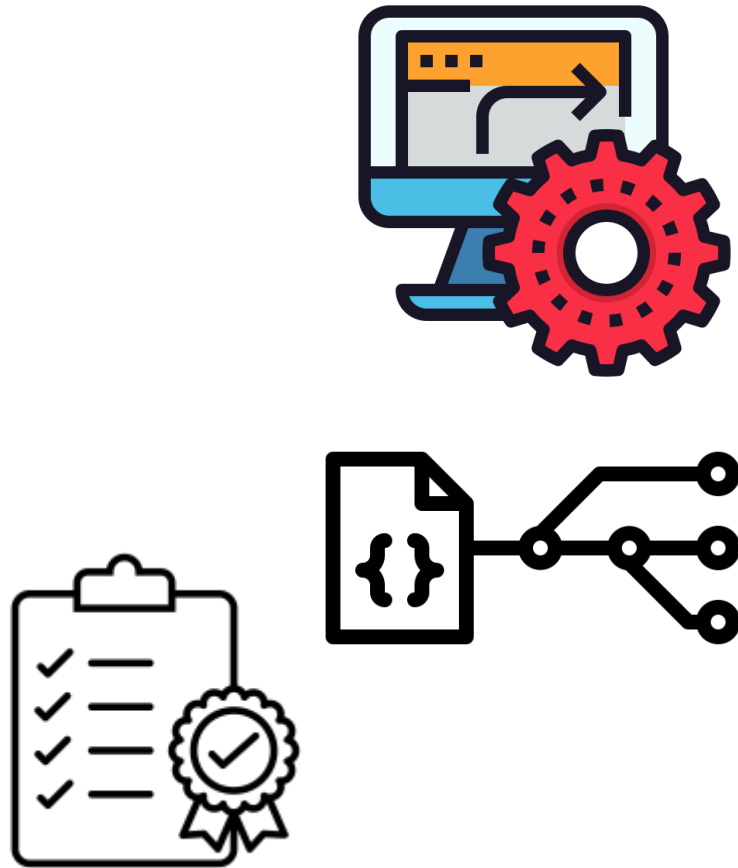
# IaC options & tools

- Azure Bicep
- Terraform
- Ansible
- AWS CDK
- Pulumi



# Declaring resources as IaC

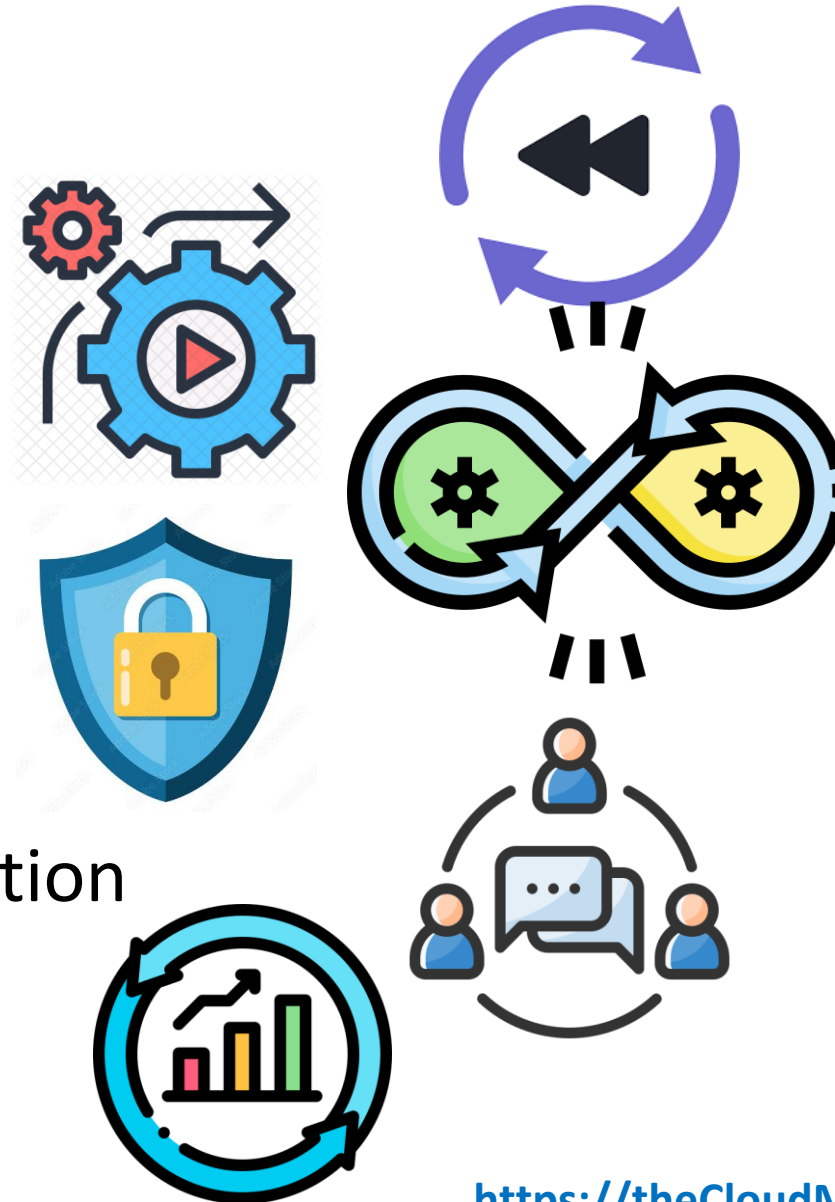
- Consistency and repeatability
- Automation
- Security Testing
- Version Control
- Compliance





# DevSecOps principles

- Shift Left
- Automation
- CI / CD
- Security as Code
- Collaboration and Communication
- Continuous Improvement



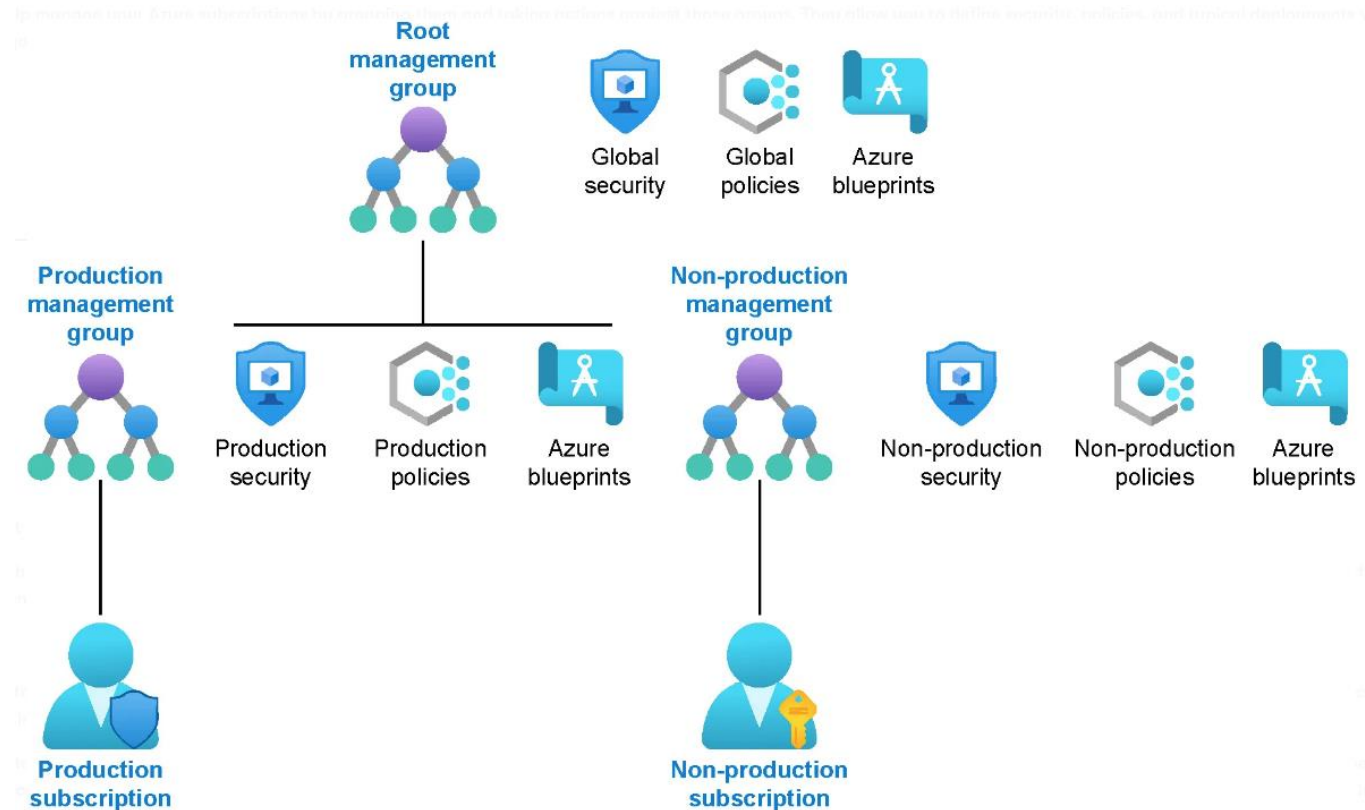
# Policies & Governance

- Security Compliance
- DevOps Practices
- Risk Management
- Continuous Monitoring
- Compliance Auditing

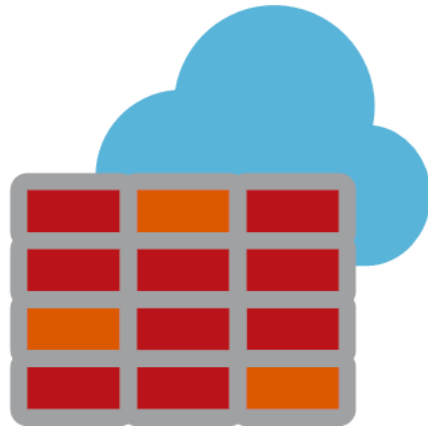
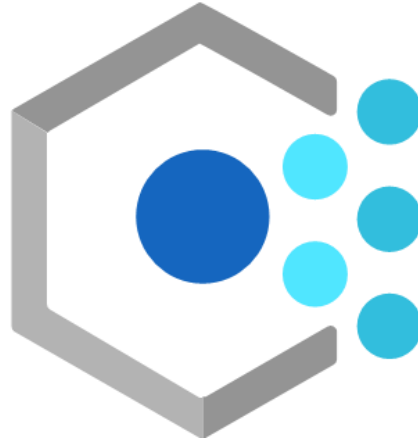


# Organizing cloud resources

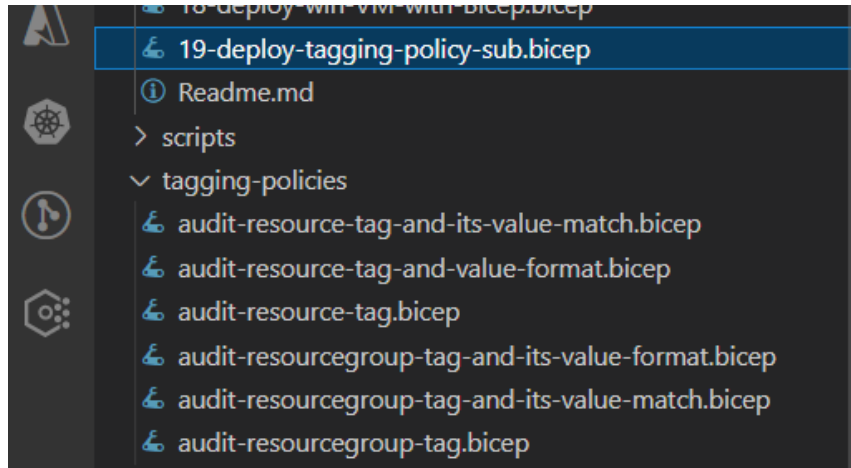
- Resource Governance
- Management scopes
- IaC management options
- Modules, ACR, Template Specs



# Use cases and Demo



# Tag Governance



## Tag Governance-1.0.0

Initiative compliance

[View definition](#) [Edit assignment](#) [Assign to another scope](#) [Delete assignment](#) [Create Remediation Task](#) [Create exemption](#)

Compliance state ⓘ



Non-compliant

Overall resource compliance ⓘ

0%

0 out of 31

Resources by compliance state ⓘ



0 - Compliant

31 - Non-compliant

Non-compliant policies ⓘ

10

out of 10

**Policies** Non-compliant resources Events

Filter by policy name or definition ID...

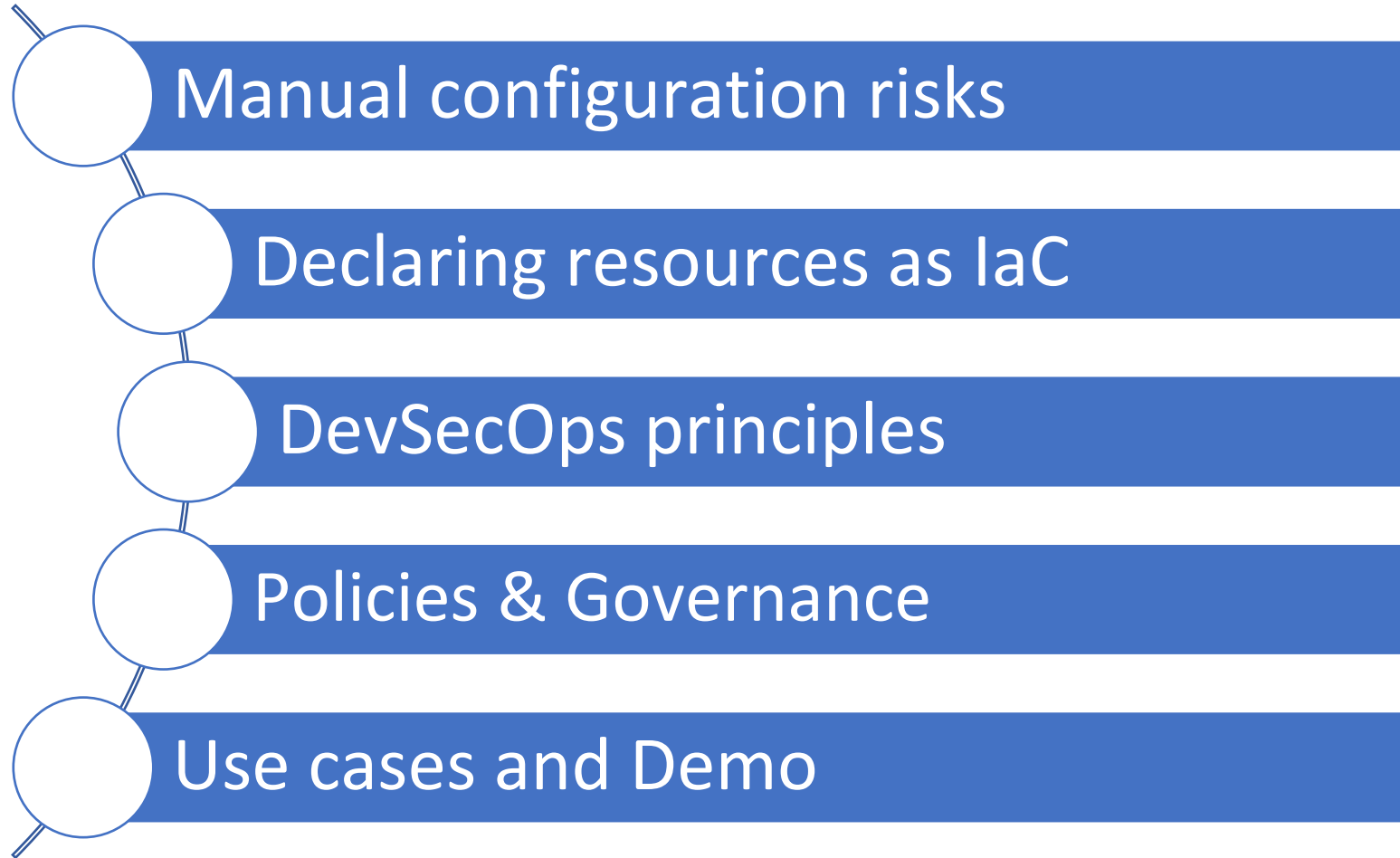
All compliance states

Name	Effect Type	Compliance state	Non-Compliant Resources
<a href="#">Audit a tag on resources</a>	Audit	Non-compliant	24
<a href="#">Audit a tag and its value format on resources</a>	Audit	Non-compliant	24
<a href="#">Audit a tag and its value match on resources</a>	Audit	Non-compliant	24
<a href="#">Audit a tag and its value format on resources</a>	Audit	Non-compliant	24
<a href="#">Audit a tag on resources</a>	Audit	Non-compliant	24
<a href="#">Audit a tag and its value match on resource groups</a>	Audit	Non-compliant	7
<a href="#">Audit a tag and its value format on resource groups</a>	Audit	Non-compliant	7
<a href="#">Audit a tag on resource groups</a>	Audit	Non-compliant	7
<a href="#">Audit a tag on resource groups</a>	Audit	Non-compliant	7
<a href="#">Audit a tag and its value format on resource groups</a>	Audit	Non-compliant	7





# What we covered

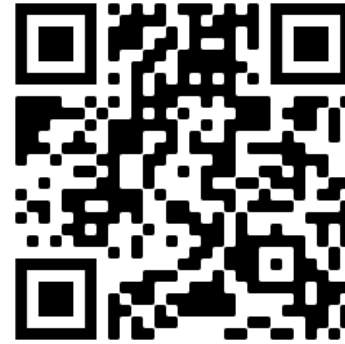


# References

Azure Bicep – First Look course 🎧



Learn Bicep – GitHub



AWESOME Azure Bicep 📄



AWESOME Azure Policy



# Thank you !



**Elkhan Yusubov**

Speaker | Author | Cloud Architect  
Founder at #cloudmarathoner

<https://cloudlunchlearn.com/weeklysessions>

<https://theCloudMarathoner.com>   