Azure Governance and Compliance Crash Course

Use Azure Policy to Enforce Organization Standards and Azure Best Practices

December/2022

Reza Salehi

Cloud Consultant and Trainer

@zaalion

Microsoft CERTIFIED Trainer

Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

Microsoft CERTIFIED CYBERSECURITY ARCHITECT EXPERT

Course Overview

Course Repository

https://github.com/zaalion/oreilly-policy-governance

Azure Governance and Compliance

- Importance of Governance and Compliance
- Azure Policy
- Azure Built-in Policies
- Creating Custom Policy Definitions
- Azure Policy Initiatives

Azure Governance

“Governance provides mechanisms and processes to maintain control over your applications and resources in Azure. It involves planning your initiatives and setting strategic priorities. ”

Microsoft

Azure Governance

Making sure your Azure resources are created and maintained according to company standards, Azure cloud best practices, or comply with government regulations such as EU GDPR.

Azure | Product documentation | Architecture | Learn Azure | Develop | Resources | Portal | Free account

Azure compliance documentation

If your organization needs to comply with legal or regulatory standards, start here to learn about compliance in Azure.

Compliance offerings

Global
- CIS benchmark
- CSA STAR Attestation
- CSA STAR Certification
- CSA STAR self-assessment
- SOC 1
- SOC 2
- SOC 3

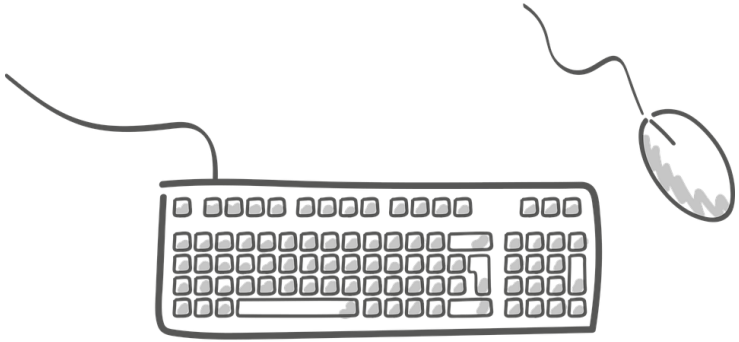
Global
- ISO 20000-1
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- ISO 9001
- WCAG

US government
- CJIS
- CMMC
- CNSSI 1253
- DFARS
- DoD IL2
- DoD IL4
- DoD IL5
- DoD IL6
- DoE 10 CFR Part 810
- EAR
- FedRAMP
- FIPS 140

US government
- ICD 503
- IRS 1075
- ITAR
- JSIG
- NDAA
- NIST 800-161
- NIST 800-171
- NIST 800-53
- NIST 800-63
- NIST CSF
- Section 508 VPATs
- StateRAMP

See reference

Demo



- Exploring Azure Compliance portal (PCI DSS, EU GDPR)

Azure Governance

- Function Apps are accessed only via HTTPS
- Azure Storage Accounts only allow AAD authentication
- API Management to disallow public network access
- Azure Cosmos DB accounts should have firewall rules
- Azure Cosmos DB should use CMKs to encrypt data at rest

Azure Governance

- User data should not be stored outside North America
- Developers are not allowed to create VMs in the DEV subscription
- Make sure the resource location matches its resource group location
- Specify a set of VM sizes that your team can deploy

Azure Policy

"Azure Policy helps to enforce organizational standards and to assess compliance at-scale."

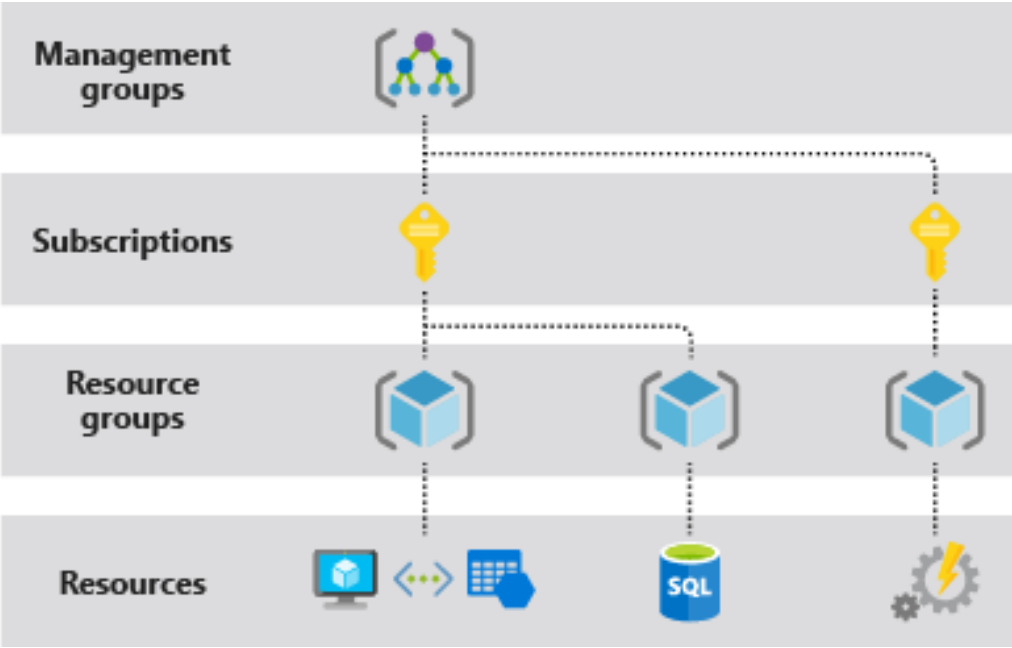
Microsoft

Azure Policy Assignment Steps

- Choose the right built-in **policy definition** for your task.
- If no built-in definition, **create a custom policy**
- Determine the **scope** for the policy
- **Assign** the policy definition to the desired scope

Azure Policy Scope

- Azure Subscription
- Azure Resource Group



See reference

Azure Policy Definition Structure

- Type
- Display name, description
- Mode
- Metadata
- Parameters
- Policy rule (logical evaluation, effect)

See reference

Audit virtual machines without disaster recovery configured

Policy definition

Assign | Edit definition | Duplicate definition | Delete definition | Export definition

Essentials

Name	: Audit virtual machines without disaster recovery configured	Definition location	: --
Description	: Audit virtual machines which do not have disaster recovery configured. To learn...	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/0015ea4d-51ff-4ce3-8d...
Available Effects	: AuditIfNotExists	Type	: Built-in
Category	: Compute	Mode	: All

Definition | Assignments (0)

```
{
  "properties": {
    "displayName": "Audit virtual machines without disaster recovery configured",
    "policyType": "BuiltIn",
    "mode": "All",
    "description": "Audit virtual machines which do not have disaster recovery configured. To learn more about disaster recovery, visit https://aka.ms/a
    "metadata": {
      "version": "1.0.0",
      "category": "Compute"
    },
    "parameters": {},
    "policyRule": {
      "if": {
        "field": "type",
        "in": [
          "Microsoft.Compute/virtualMachines",
          "Microsoft.ClassicCompute/virtualMachines"
        ]
      },
      "then": {
```

Azure Policy Effect

- Each policy definition in Azure Policy has a single effect.
- Determines what happens when the policy rule is evaluated
- The effects behave differently if they are for a *new resource*, an *updated resource*, or an *existing resource*

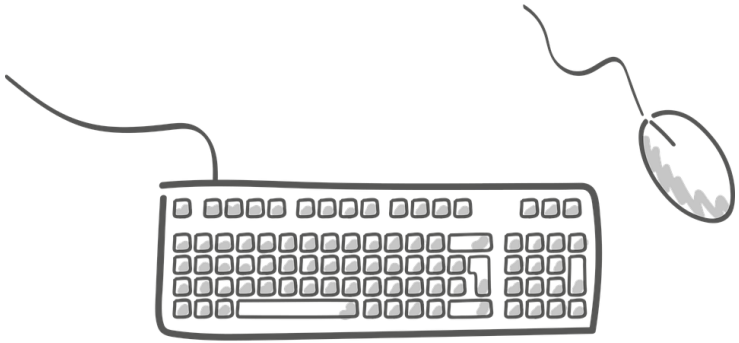
See reference

Azure Policy Effect

- Append
- Audit
- AuditIfNotExists
- Deny
- DeployIfNotExists
- Disabled
- Modify

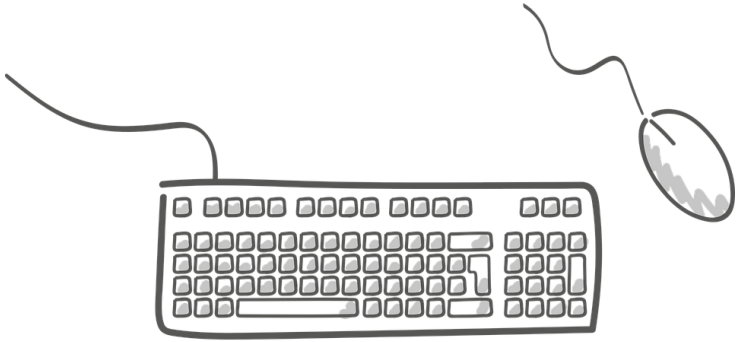
See reference

Demo



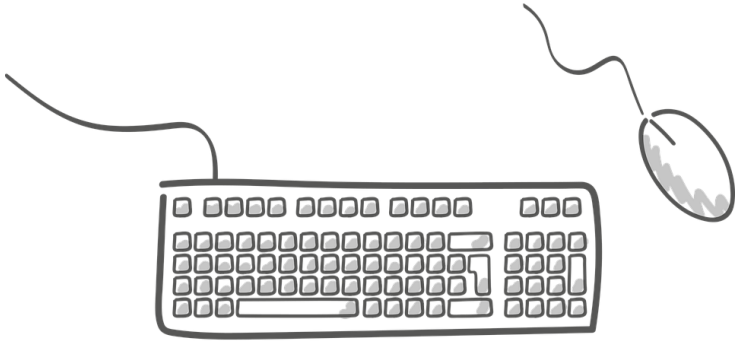
- Exploring the Azure Policy overview page

Demo



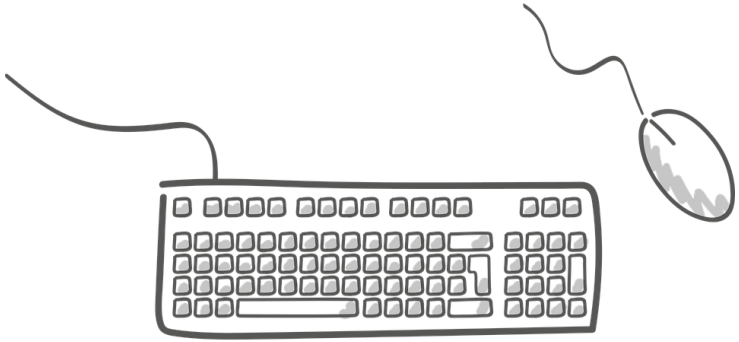
- Built-in general Policy definitions

Demo



- Policy definitions for specific resource types

Demo



- Identifying the right built-in policy for your scenario

Azure Policy Assignment Structure

- Display name, description
- Metadata
- Enforcement mode
- Excluded scopes
- Policy definition
- Non-compliance messages
- Parameters
- Identity

See reference

All services > Policy

Policy | Assignments

Search (Ctrl+/)

- Overview
- Getting started
- Compliance
- Remediation
- Events

Authoring

- Definitions
- Assignments
- Exemptions

Assign policy | Assign initiative | Refresh

Scope: Pay-As-You-Go

Definition type: All definition types

Search: Filter by name or ID...

Now create custom non-compliance messages for policy assignments. Learn more https://aka.ms/policyassignmentnoncompliancemessage

Total Assignments	Initiative Assignments	Policy Assignments
1	1	0

Assignment name	Scope	Type
ASC Default (subscription: 19969c81-e8ff-4585-8c2f-3f196b588227)	Pay-As-You-Go	Initiative

All services >

Policy

Search (Ctrl+/)

- Overview
- Getting started
- Compliance
- Remediation
- Events

Authoring

- Definitions
- Assignments
- Exemptions

Scope

Pay-As-You-Go

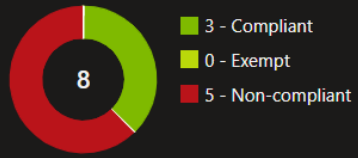
Get notified of compliance state changes! Use event-based architecture to react to notifications with an Azure Function, Logic App, or any other supported event handler. Learn more https://aka.ms/policyPlusEventGrid

Overall resource compliance

38%

3 out of 8

Resources by compliance state



Non-compliant initiatives

1

out of 1

LEARN MORE

Learn about Policy

Onboarding tutorial

Non-compliant policies

38

out of 203

Name	Scope	Compliance state	Resource compli...	Non-Compliant Reso...	Non-compliant polici...
ASC Default (subscription...	Pay-As-You-Go	Non-compliant	38% (3 out of 8)	5	38

View all

Built-in Azure Policy Definitions

API Management

App Service

Azure Databricks

Bot Service

Cognitive Services

Compute

Cosmos DB

General

Key Vault

Network

Service Bus

SQL

Storage

Tags

See reference

Policy | Definitions

Search (Ctrl+/)

Overview
Getting started
Compliance
Remediation
Events

Authoring

Definitions
Assignments
Exemptions

Policy definition | Initiative definition | Export definitions | Refresh

Scope: Pay-As-You-Go

Definition type: All definition types

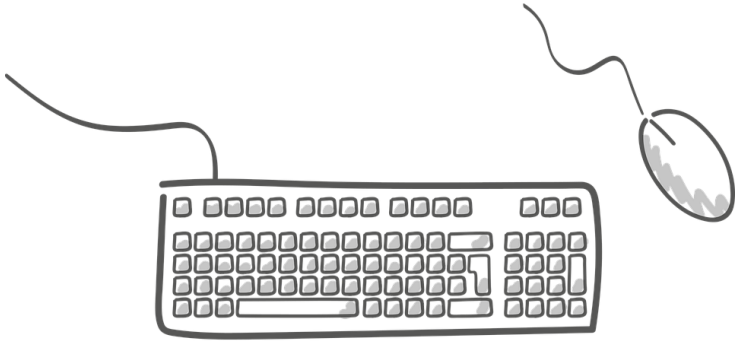
Category: All categories

Search: Filter by name or ID...

Now export your definitions and assignments to GitHub and manage them using actions! Click on 'Export definition' menu option. Learn more

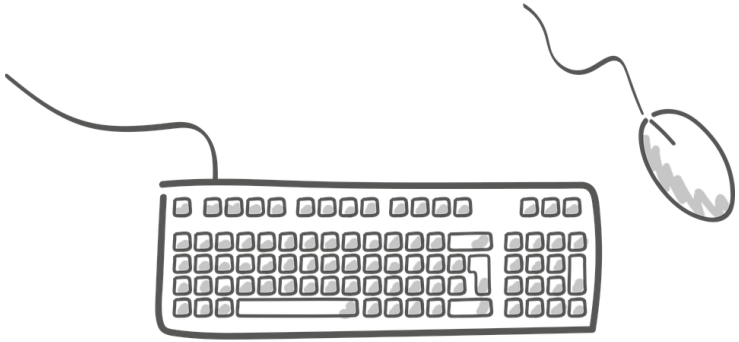
Name	Definition location	Policies	Type	Definition type
Audit virtual machines without disaster recovery confi...			BuiltIn	Policy
Vulnerability assessment should be enabled on your S...			BuiltIn	Policy
SQL Server Integration Services integration runtimes ...			BuiltIn	Policy
[Preview]: Configure VMSS created with Shared Image...			BuiltIn	Policy
Private endpoint connections on Batch accounts shou...			BuiltIn	Policy
Azure Backup should be enabled for Virtual Machines			BuiltIn	Policy
Configure a private DNS Zone ID for table groupID			BuiltIn	Policy
[Preview]: Azure Security agent should be installed on...			BuiltIn	Policy
Cognitive Services accounts should restrict network a...			BuiltIn	Policy
Azure Kubernetes Service Private Clusters should be e...			BuiltIn	Policy
Audit Linux machines that have the specified applicati...			BuiltIn	Policy

Demo



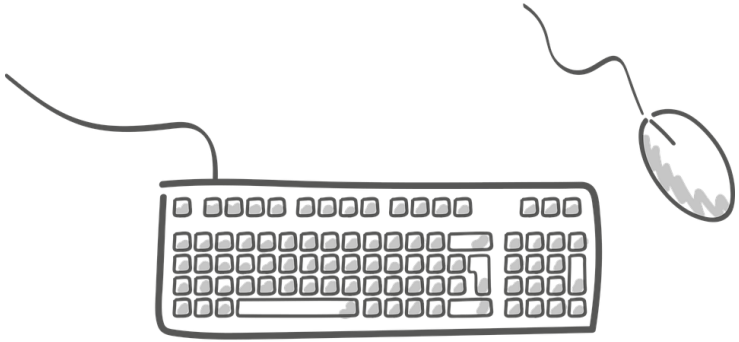
- Using policies to limit deployment locations (regions)
- Using policies to limit allowed resource types
- Using policies to enforce resource tagging
- Using policies to enforce proper resource logging (resource log)

Demo



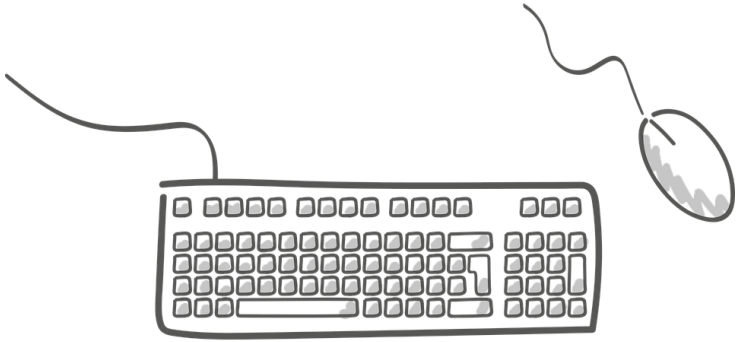
- Storage accounts should restrict network access using virtual network rules
- Secure transfer to storage accounts should be enabled
- Storage accounts should be limited by allowed SKUs
- Storage accounts should prevent shared key access
- Storage accounts should disable public network access
- Storage accounts should have the specified minimum TLS version

Demo



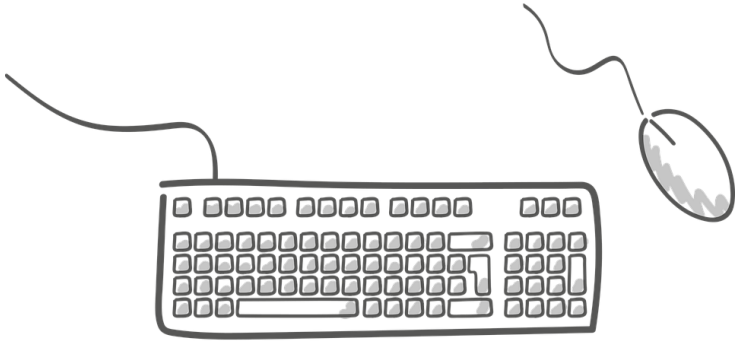
- Azure Cosmos DB should disable public network access
- Azure Cosmos DB accounts should have firewall rules
- Configure CosmosDB accounts with private endpoints
- Enable Azure Cosmos DB throughput policy

Demo



- Function apps should use managed identity
- Configure Function apps to turn off remote debugging
- Function apps should only be accessible over HTTPS
- Function apps should use latest 'HTTP Version'

Demo



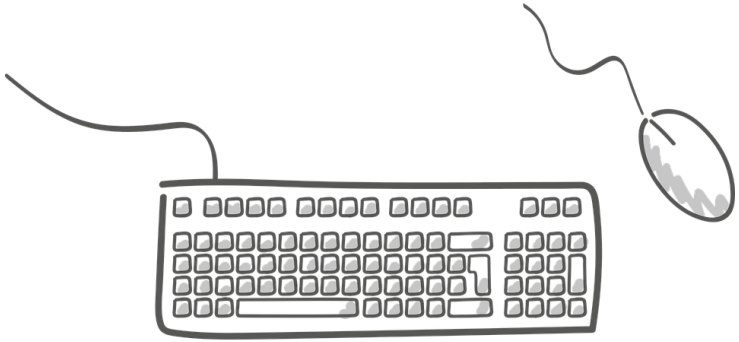
- Azure Service Bus namespaces should use private link
- Service Bus Namespaces should disable public network access
- Resource logs in Service Bus should be enabled

Creating Custom Policy Definitions

- When there is **no built-in policy** matching your needs
- **Create** a new policy definition
- **Assign** the policy to desired scopes.
- **Store the policy definition** JSON in source control

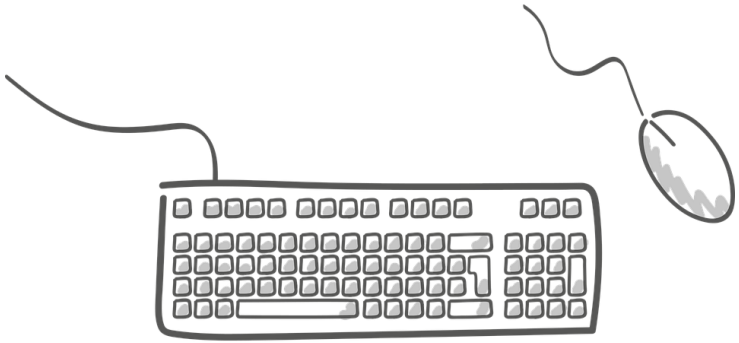
See reference

Demo



- Creating a new custom policy definition

Demo



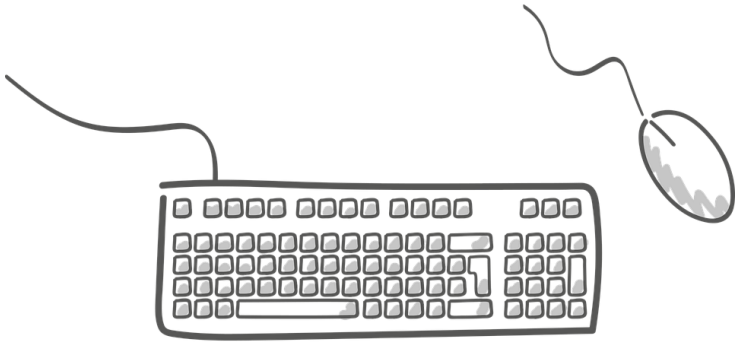
- Assigning our new custom policy definition

Azure Policy Exemptions

“The Azure Policy exemptions feature is used to exempt a resource hierarchy or an individual resource from evaluation of initiatives or definitions.“

Microsoft

Demo



- Azure Policy Exemptions

Azure Policy Initiative

“An Azure Policy initiative is a collection of Azure Policy definitions, or rules, that are grouped together towards a specific goal or purpose. “

Microsoft

Policy | Definitions

Search (Ctrl+/)

- Overview
- Getting started
- Compliance
- Remediation
- Events

Authoring

- Definitions
- Assignments
- Exemptions

Policy definition | Initiative definition | Export definitions | Refresh

Scope: Pay-As-You-Go

Definition type: Initiative

Category: All categories

Search: Filter by name or ID...

Now export your definitions and assignments to GitHub and manage them using actions! Click on 'Export definition' menu option. Learn more

Name	Definition location	Policies	Type	Definition type
NIST SP 800-171 Rev. 2		247	BuiltIn	Initiative
Audit machines with insecure password security settings		9	BuiltIn	Initiative
Deploy Windows Azure Monitor Agent with user-assigne...		5	BuiltIn	Initiative
IRS1075 September 2016		60	BuiltIn	Initiative
Configure Linux machines to run Azure Monitor Agent an...		4	BuiltIn	Initiative
Deploy prerequisites to enable Guest Configuration polici...		4	BuiltIn	Initiative
NIST SP 800-53 Rev. 5		955	BuiltIn	Initiative
CIS Microsoft Azure Foundations Benchmark v1.1.0		86	BuiltIn	Initiative
Azure Security Benchmark		203	BuiltIn	Initiative
Enable Azure Monitor for VMSS with Azure Monitoring A...		6	BuiltIn	Initiative
[Preview]: Australian Government ISM PROTECTED		55	BuiltIn	Initiative

Azure | Product documentation | Architecture | Learn Azure | Develop | Resources | Portal | Free account

Azure compliance documentation

If your organization needs to comply with legal or regulatory standards, start here to learn about compliance in Azure.

Compliance offerings

Global
- CIS benchmark
- CSA STAR Attestation
- CSA STAR Certification
- CSA STAR self-assessment
- SOC 1
- SOC 2
- SOC 3

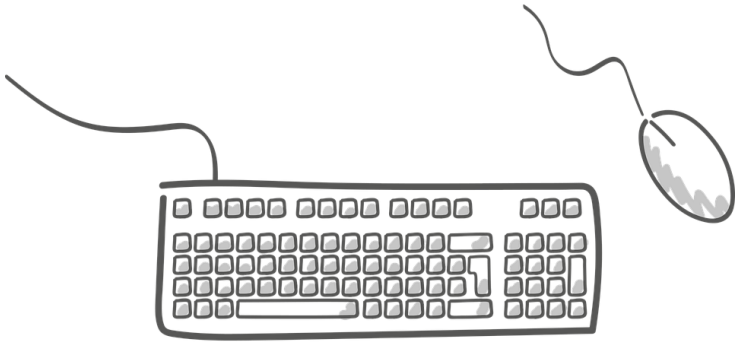
Global
- ISO 20000-1
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- ISO 9001
- WCAG

US government
- CJIS
- CMMC
- CNSSI 1253
- DFARS
- DoD IL2
- DoD IL4
- DoD IL5
- DoD IL6
- DoE 10 CFR Part 810
- EAR
- FedRAMP
- FIPS 140

US government
- ICD 503
- IRS 1075
- ITAR
- JSIG
- NDAA
- NIST 800-161
- NIST 800-171
- NIST 800-53
- NIST 800-63
- NIST CSF
- Section 508 VPATs
- StateRAMP

See reference

Demo



- Exploring built-in policy initiatives

Course Repository

https://github.com/zaalion/oreilly-policy-governance

O'REILLY®

Thank you!

Reza Salehi

@zaalion