UbuCon India 25

# OSCAL & GRC Automation

Balachandran Sivakumar | Co-founder, CISOGenie

Qualcomm Canonical IT'S FOSS INDIAN INSTITUTE OF SCIENCE भारतीय विज्ञान संस्थान

# Agenda

- What is GRC?
- The Compliance Chaos
- Enter OSCAL – Machine-readable Security Controls
- OSCAL Models: Catalog → Profile → Component → SSP
- From Baseline to Assessment Plan & Results
- Policy-as-Code with OPA/Rego
- Continuous Compliance Loop
- Demo & Real-world Wins
- Q&A

# GRC - The Lesser Known Component Of Cybersecurity

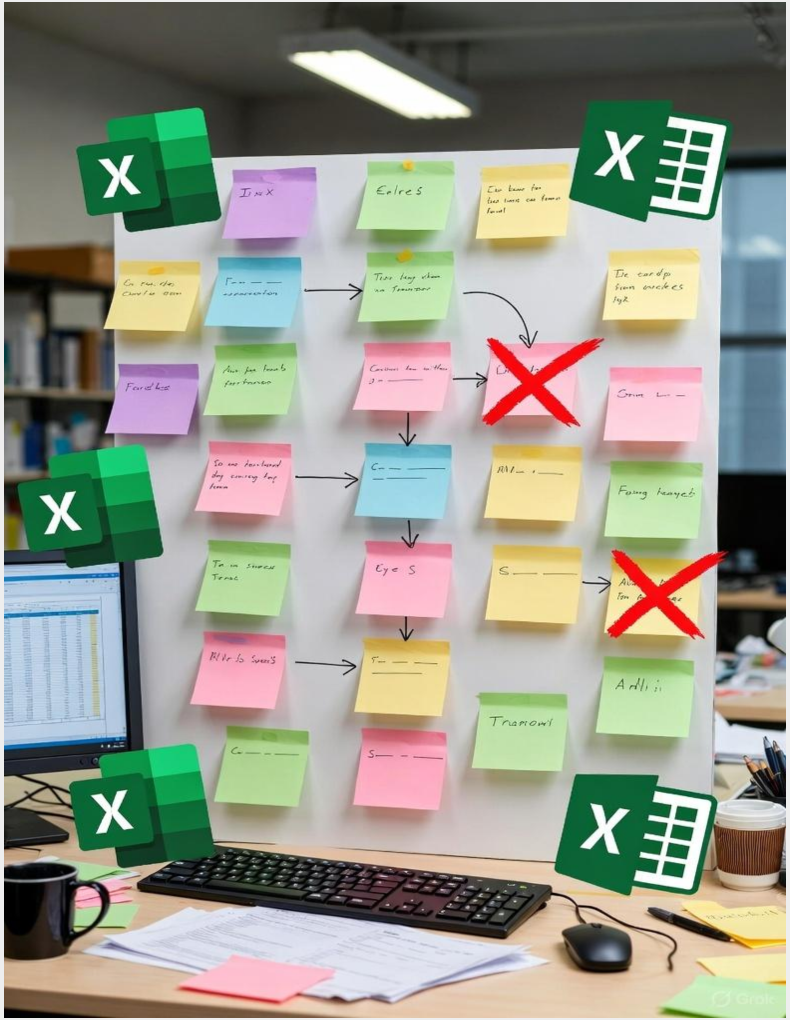
Governance, Risk & Compliance

- **Governance**: Policies, roles, accountability
- **Risk**: Identify, assess, mitigate
- **Compliance**: Meet laws, standards, contracts

**GRC is the backbone of trust and security**

# The Compliance Chaos

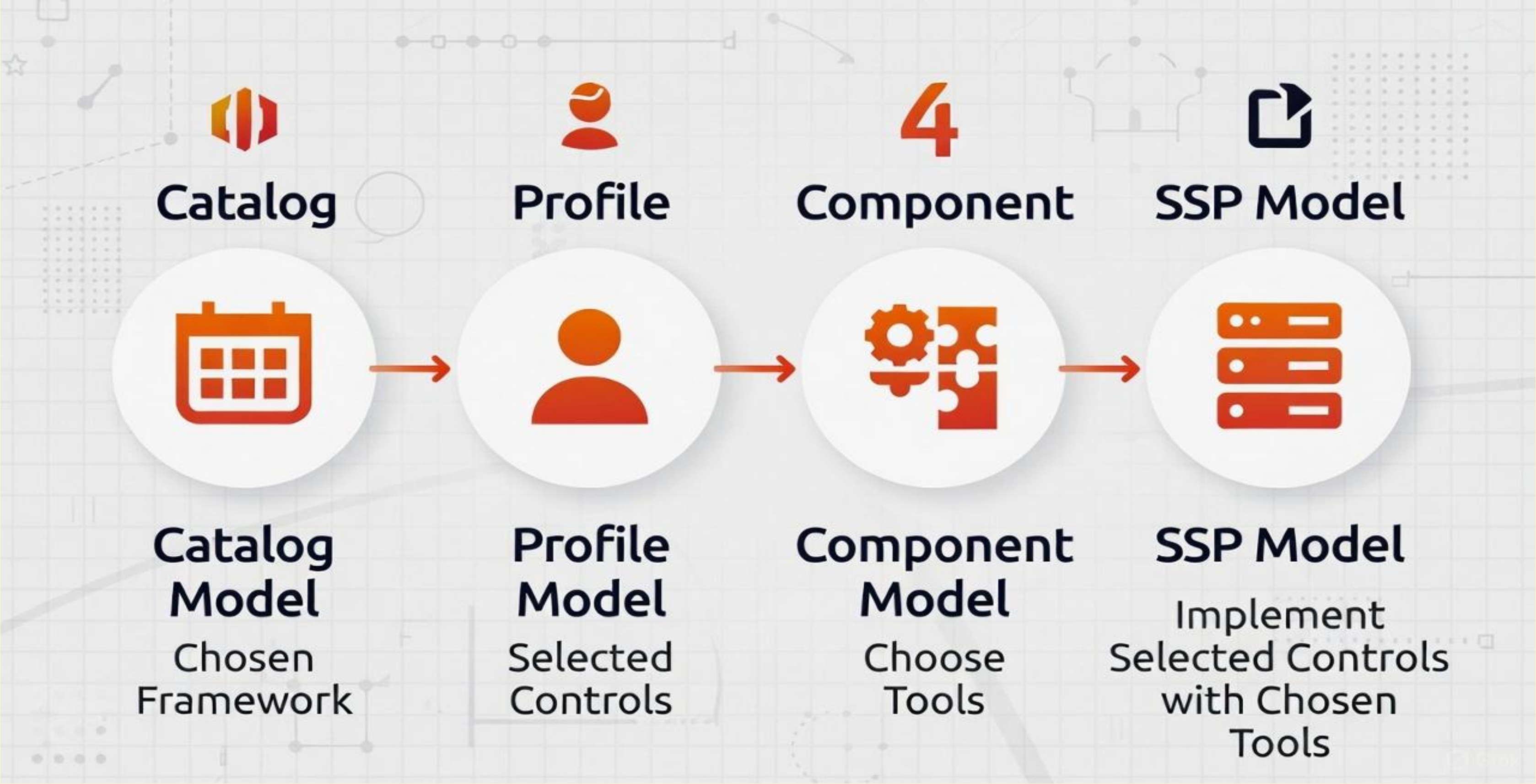
Siloed tools, teams and processes,
Point-in-time snapshot evidences,
Manual and cumbersome



# OSCAL

NATIONAL INSTITUTE OF
NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Open Security Controls Assessment Language
uuid{
title{
params" 00Ue>#oleeen(>>(valees))
prop}
label'
values';
flag}
constraints';
constrainttype';
datatype';
description values';
description);
Grok

# OSCAL Models



Catalog → Profile → Component → SSP Model

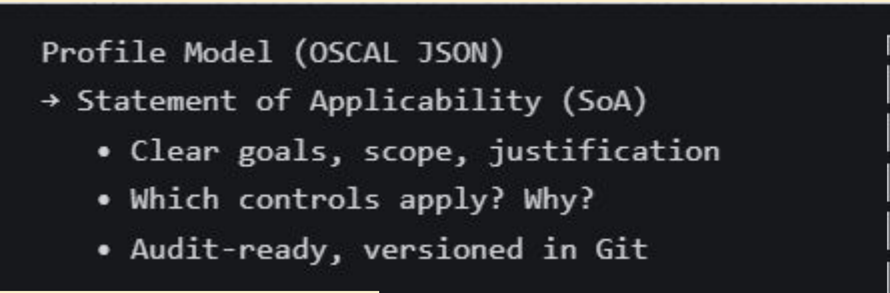
**Catalog Model**
Chosen Framework

**Profile Model**
Selected Controls

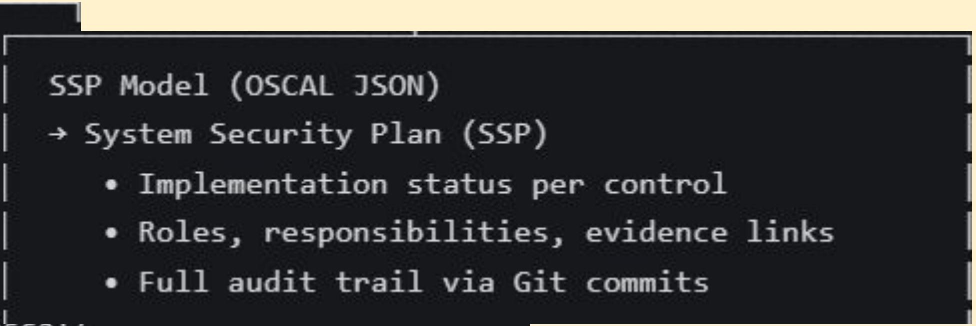
**Component Model**
Choose Tools

**SSP Model**
Implement Selected Controls with Chosen Tools

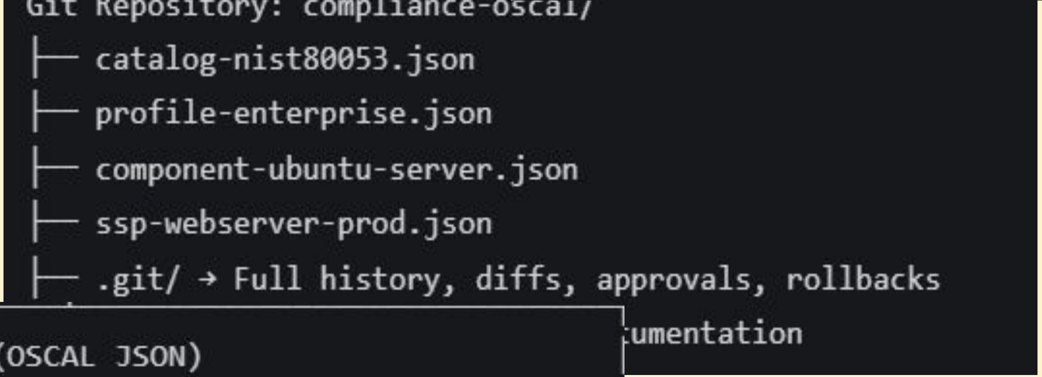
# Baseline Achieved!



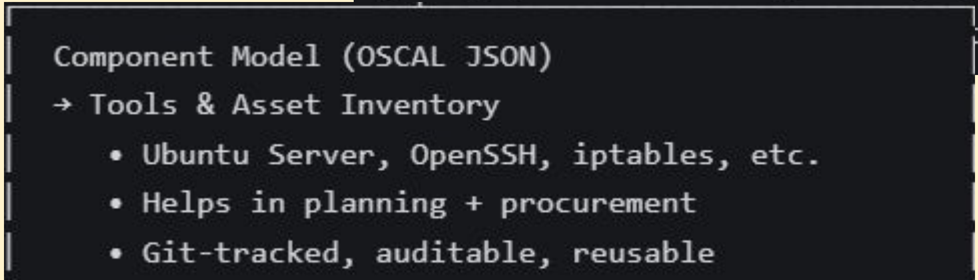
```
Profile Model (OSCAL JSON)
→ Statement of Applicability (SoA)
   • Clear goals, scope, justification
   • Which controls apply? Why?
   • Audit-ready, versioned in Git
```



```
SSP Model (OSCAL JSON)
→ System Security Plan (SSP)
   • Implementation status per control
   • Roles, responsibilities, evidence links
   • Full audit trail via Git commits
```



```
Git Repository: compliance-oscal/
├── catalog-nist80053.json
├── profile-enterprise.json
├── component-ubuntu-server.json
├── ssp-webserver-prod.json
├── .git/ → Full history, diffs, approvals, rollbacks
                                    umentation
```

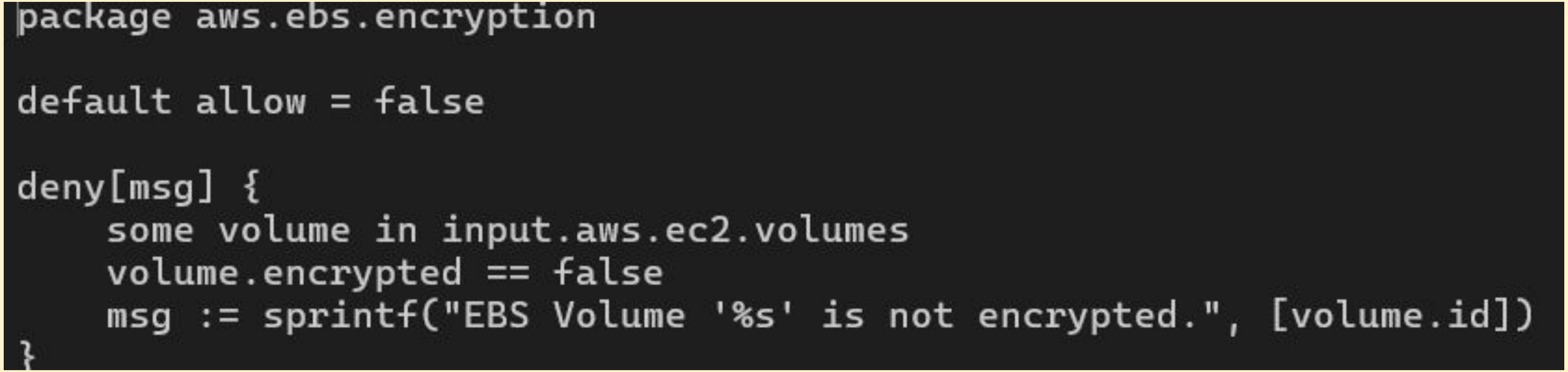


```
Component Model (OSCAL JSON)
→ Tools & Asset Inventory
   • Ubuntu Server, OpenSSH, iptables, etc.
   • Helps in planning + procurement
   • Git-tracked, auditable, reusable
```

# Assessments: OSCAL + OPA/Rego

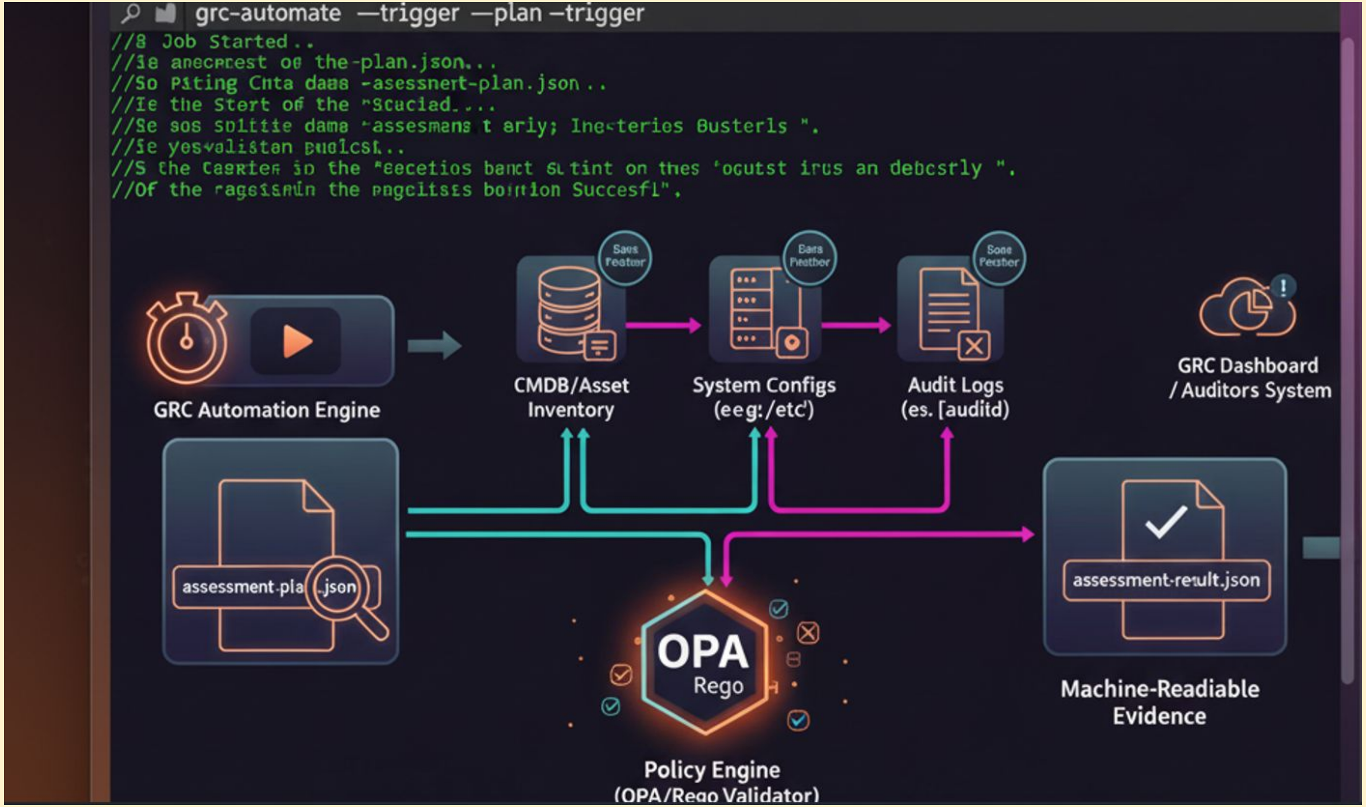
Assessment layer has 2 models

- Assessment Plan - How will you test? (OPA/Rego scripts?)
- Assessment Result - What did you find? (status & evidence)



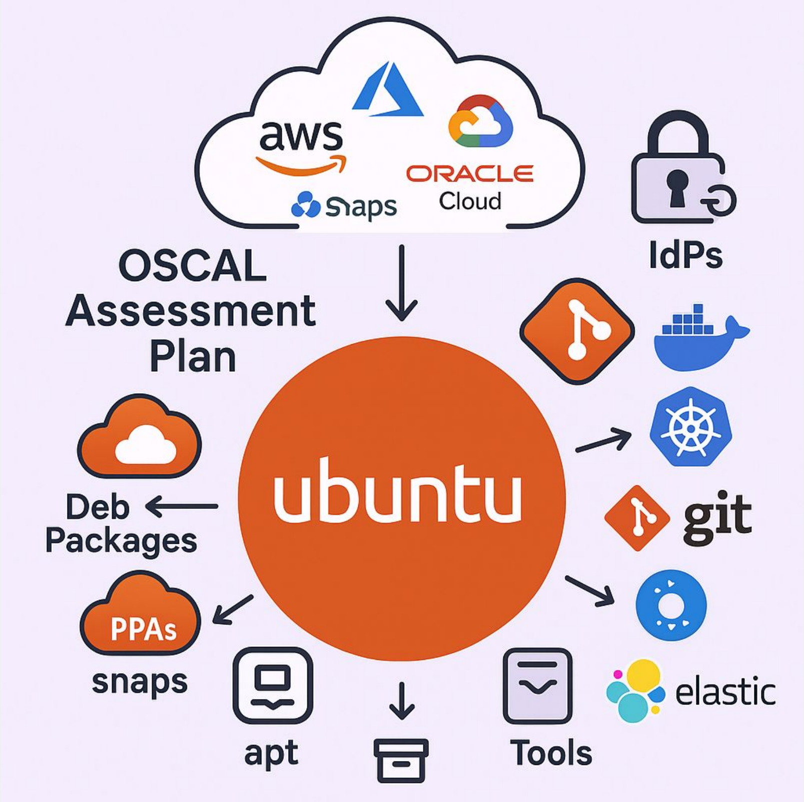
```
package aws.ebs.encryption

default allow = false

deny[msg] {
    some volume in input.aws.ec2.volumes
    volume.encrypted == false
    msg := sprintf("EBS Volume '%s' is not encrypted.", [volume.id])
}
```

# Continuous Compliance



```
grc-automate —trigger —plan —trigger
//8 Job Started..
//ie anecrrest oe the-plan.json...
//So Piting Cnta daas -asessnert-plan.json..
//Ie the Stert of the "Scuciad....
//Se sos spltitie dama "assesmans t ariy; Inesteries Busterls ".
//ie yesvalistan puelcst...
//S the Casrter ip the "eecetios banct st tint on thes 'ocutst irus an debcsrly ".
//Of the ragsismin the pngcitsts boirtion Succesfl".
```

# Ubuntu - The Ecosystem behind it all!



UbuCon India 25

# Thank You!

Qualcomm

Canonical

IT'S FOSS

INDIAN INSTITUTE OF SCIENCE
भारतीय विज्ञान संस्थान