Objective: Simulate a few misconfiguration in Cloud and then strategize the fix and align this with GRC of organization.

Tool Used: Terraform, Azure Cloud, Microsoft Defender for Cloud, ISO mapping, and **OpenRMF** as the central open-source GRC tool.

Step 1: Simulate Misconfigured Azure Resources

Use Terraform/Azure Portal to deploy the following:

Purpose: Demonstrate real-world risks and misconfigurations.

Resource	**Misconfiguration**	**Risk**
Azure VM	RDP (3389) open to internet	High – Brute-force attack
Azure Storage Account	Public blob access enabled	High – Data leakage
Azure SQL Database	No firewall rules, weak admin password	Critical – Unauthorized access
Azure Key Vault	Access policies allow all users	High – Secrets exposure
Azure App Service	HTTPS not enforced	Medium – Data in transit at risk
Azure Function	Anonymous access enabled	High – Unauthenticated execution
Azure NSG	0.0.0.0/0 allowed on multiple ports	High – Network exposure
Azure Cosmos DB	Firewall disabled, no IP restrictions	High – Data exfiltration
Azure Logic Apps	No IP filtering or authentication	Medium – Workflow abuse
Azure Container Registry	Admin user enabled, no RBAC	High – Image tampering risk

Step 2: Enable Microsoft Defender for Cloud

- Enable Defender for Cloud at the subscription level.
- Review **Secure Score** and **Recommendations**.
- Identify flagged misconfigurations from Step 1.

Step 3: Map Findings to ISO 27001 / 27017 Controls

Purpose: Show how cloud misconfigurations impact compliance posture.

Misconfiguration	**ISO 27001 Control**	**ISO 27017 Control**
Open RDP port	A.13.1.1	9.4.1
Public blob access	A.9.1.2	9.1.3
Weak DB security	A.9.2.3	12.1.5
Key Vault exposure	A.10.1.1	10.1.1
No HTTPS on App Service	A.13.2.3	10.1.2
Anonymous Azure Function	A.9.4.1	9.1.1
NSG open to all	A.13.1.1	9.4.1
Cosmos DB firewall off	A.13.1.3	9.4.2
Logic Apps no auth	A.9.2.1	9.1.1
ACR admin enabled	A.9.2.3	12.1.5

Step 4: Introduce Risk Management

Use **Microsoft Defender for Cloud** and **OpenRMF**

- Identify risks
- Assign severity
- Prioritize remediation

Purpose: Understand risk lifecycle and impact.

Step 5: Use OpenRMF for GRC

Purpose: Centralize GRC activities in one open-source tool.

Task	Action in OpenRMF
Log Risks	Input misconfigurations as risks
Risk Treatment	Choose Accept, Mitigate, Transfer, Avoid
Compliance Mapping	Use templates for ISO 27001/27017
POA&M Generation	Create Plan of Action and Milestones
Audit Readiness	Export reports for review and evidence

Step 6: Continuous Monitoring & Feedback

- Re-scan environment after remediation
- Update OpenRMF with new findings
- Track accepted risks and mitigation progress
- Use reports for internal audits or external compliance checks

Summary

This strategy gave me

- A **realistic simulation** for teaching or training
- A **CSPM tool (Defender for Cloud)** for posture visibility
- A **GRC tool (OpenRMF)** for managing risks and compliance
- A **framework aligned with ISO standards**