GRC Engineering 101

How I Learned To Stop Worrying and Love The Risk Register

Darryl MacLeod

HELLO
my name is

Darryl

The Problem with Traditional GRC

- Manual audits and quarterly reviews
- Static checklists
- Reactive, not proactive
- Can't keep up with rapid change

Cloud Moves Fast

- Auto-scaling and ephemeral resources
- Continuous integration and deployment
- Multi-region and multi-cloud data flow

Enter GRC Engineering

- Compliance built directly into infrastructure
- Prevents non-compliance before it happens
- Enables continuous assurance

Four Pillars of GRC Engineering

1. Automation
2. Infrastructure as Code (IaC)
3. CI/CD Integration
4. Policy as Code

Pillar 1 – Automation

- Removes human error
- Applies controls consistently at scale
- Examples: Auto-patching, config drift detection

Pillar 2 – Infrastructure as Code (IaC)

- Treat infrastructure like software
- Version control and repeatability
- Enforce secure, compliant defaults

Pillar 3 – CI/CD Integration

- Compliance checks built into pipelines
- Block insecure deployments
- Catch issues early in the development cycle

Pillar 4 – Policy as Code

- Turn compliance rules into executable logic
- Enforce continuously, not periodically
- Examples: No unencrypted storage, tagging enforcement

Traditional vs. GRC Engineering Approach

Traditional GRC	GRC Engineering
Find issues after deployment	Prevent issues at deployment
Manual audits	Automated, continuous checks
Hope teams follow policies	Embed policies as code

Benefits of GRC Engineering

- Reactive → Proactive
- Manual → Automated
- Enforcement → Enablement

Getting Started

- Pick a single compliance pain point
- Automate one small process
- Expand incrementally

Common Challenges

- “Too technical” → Partner with engineering
- “No budget” → Show ROI with quick wins
- “Auditors don’t get it” → Educate on continuous monitoring

ISO 27001:2022

- Continuous Risk Register Updates:

  Integrate Jira or ServiceNow tickets into a risk register automatically when vulnerabilities or audit findings are logged.

Compliance must be part of the system, not bolted on after.

Thank You!