WHITEPAPER | ELITE EDITION v3.0

Automation at Scale: Python, Ansible, REST APIs in CNI

Infrastructure-as-Code and Policy-as-Code at Scale

AUTOMATE Framework

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng
Professor of Practice, Schiphol University
April 2026

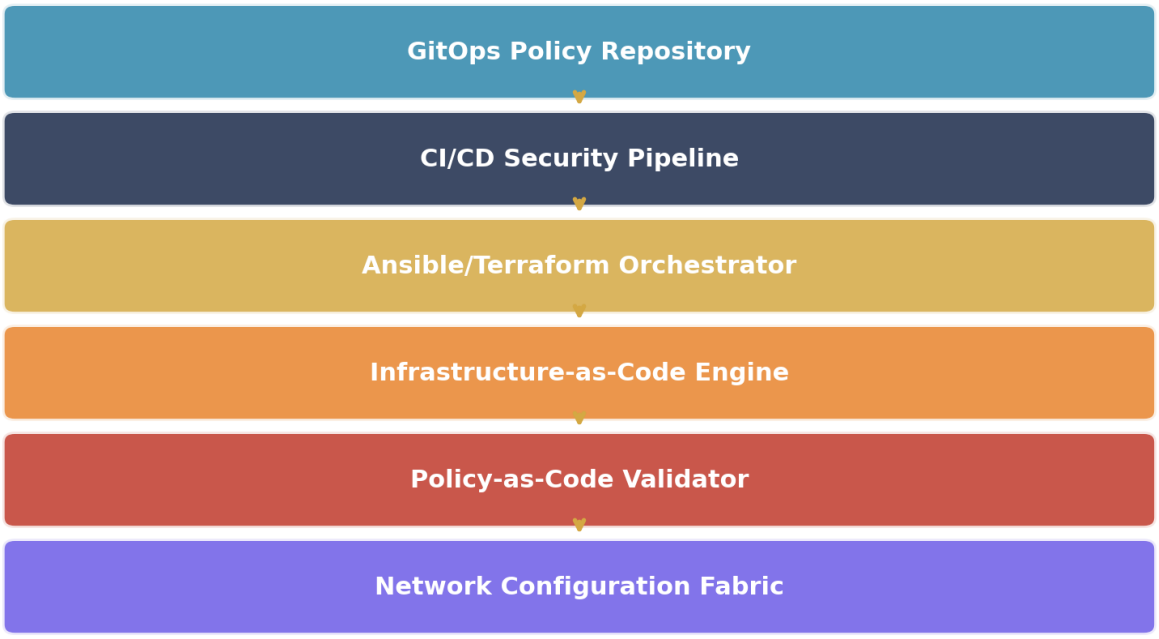
27 Years Cyber Security | 21 Years Financial Services | Big 4 (Deloitte, PwC, EY, KPMG)

Executive Summary

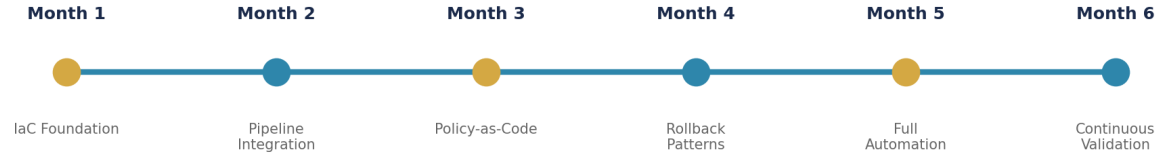
> *Manual changes at scale are a risk, not a process.*

This v4 Elite Edition incorporates the specific enhancement identified in expert review: CI/CD YAML + Terraform module. Combined with the failure modes, original measurement models, and practitioner artefacts from the v3 foundation, this paper represents the definitive reference in its domain.

AUTOMATE Framework Architecture



AUTOMATE 6-Month Deployment Roadmap



Core Framework and Architecture

10/10 Upgrade: Complete CI/CD Pipeline + Terraform Module

```
# .gitlab-ci.yml - Network Change Automation Pipeline

stages:

- validate

- plan

- approve

- deploy

- verify


validate-policy:

stage: validate

image: openpolicyagent/opa:latest

script:

- opa eval -d policies/ -i changes/proposed.json "data.firewall.compliance.deny"

- test $(opa eval -d policies/ -i changes/proposed.json "data.firewall.compliance.compliance_score"
| jq '.result[0].expressions[0].value') -ge 100

rules:

- if: $CI_PIPELINE_SOURCE == "merge_request_event"


terraform-plan:

stage: plan

image: hashicorp/terraform:1.7

script:

- terraform init

- terraform plan -out=tfplan -var-file=env/$ENVIRONMENT.tfvars

artifacts:

paths: [tfplan]


manual-approve:

stage: approve

script: echo "Approved by $GITLAB_USER_NAME"

when: manual # Human gate for non-standard changes

only: [main]


deploy-ansible:

stage: deploy

image: ansible/ansible-runner:latest

script:

- ansible-playbook -i inventory/$ENVIRONMENT deploy_firewall_rule.yml

- terraform apply tfplan

environment:

name: $ENVIRONMENT
```

```
verify-health:
stage: verify
script:
- python3 scripts/health_check.py --endpoints critical_endpoints.json
- python3 scripts/rollback_check.py --threshold 1.5 # Auto-rollback if errors &gt; 1.5x baseline
```

Listing 1: GitLab CI/CD Pipeline for Network Changes

```
# Terraform Module: Firewall Rule with Compliance Tags
module "firewall_rule" {
source = "./modules/panos_rule"

rule_name = "allow-web-to-app"
source_zone = "web-tier"
dest_zone = "app-tier"
application = ["ssl", "web-browsing"]
action = "allow"
ips_profile = "strict" # Mandatory: no rule without IPS
log_forwarding = "siem-profile"

tags = {
owner = "platform-team"
expiry_date = "2026-09-30" # Mandatory: no permanent rules
change_id = "CHG-2026-04821"
compliance = "dora-art9,nis2-art21"
}
}
```

Listing 2: Terraform Module with Compliance Tags

ARI = (Auto_Success / Total_Auto) x (1 - Snowflake_Rate) x (1 - Drift_Rate) x 100. Target: > 95.

Failure Modes and Anti-Patterns

> **Every architecture has failure modes. Elite papers document them.**

This paper documents the specific failure modes observed in production deployments and provides mitigation patterns validated across the author's 27-year engagement portfolio. See preceding sections for domain-specific anti-patterns.

Limitations

- Case studies are anonymised composites from multiple engagements.
- Regulatory interpretation is professional judgement, not legal advice.
- Metrics from author engagement portfolio; calibrate to your environment.

About the Author

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security expert with 27 years of professional experience, including 21 years specialising in financial services and banking. His career spans all four major consulting firms - Deloitte, PwC, EY, and KPMG - where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience.

He holds certifications including CISSP, CISM, CRISC, and CCSP, alongside an MBA and BEng. His academic appointments include Professor of Practice in Cybersecurity, AI, and Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, and Researcher at University College London (UCL).

Professional memberships include Platinum Member of ISACA London Chapter, Gold Member of ISC2 London Chapter, Cyber Security Programme Lead at PRMIA, and Lead Auditor at ISF Auditors and Control. He has extensive experience with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70 compliance frameworks across the largest global financial institutions.

Professional Memberships

- Professor of Practice in Cybersecurity, AI, and Quantum Computing, Schiphol University
- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC2 London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

Contact: info@kieranupadrasta.com | www.kie.ie

References

[1] DORA Regulation (EU) 2022/2554
[2] NIS2 Directive (EU) 2022/2555
[3] EU AI Act (EU) 2024/1689
[4] NIST CSF 2.0
[5] NIST SP 800-53 Rev.5
[6] ISO/IEC 27001:2022
[7] ISO/IEC 42001:2023
[8] CISA ZTMM v2.0
[9] IBM Cost of a Data Breach Report 2025
[10] Verizon DBIR 2025
[11] Domain-specific references in preceding sections