Infrastructure as Code for Repeatable, Auditable Environments

Adoption of infrastructure-as-code practices that replace manual configuration with declarative, version-controlled templates, enabling repeatable deployments, drift detection, and compliance-as-code.

PRACTICE

DevSecOps and Platform Engineering

CLIENT PROFILE

IT operations team managing multiple environments that need repeatable, version-controlled infrastructure provisioning with drift detection and compliance enforcement

Challenge

- Manually configured environments with undocumented snowflake configurations
- Configuration drift between development, staging, and production environments
- No version control or approval workflow for infrastructure changes

Approach

- Codify existing infrastructure as declarative templates (Terraform, Ansible, or ARM/CloudFormation)
- Implement GitOps workflow with pull request reviews and automated plan/apply pipelines
- Deploy drift detection and automated remediation for compliance-critical configurations
- Create reusable module libraries for standardized infrastructure patterns

Typical Outcomes

- Repeatable, consistent environments provisioned in minutes instead of days
- Complete change history with approval workflows and rollback capability
- Automated compliance validation reducing manual audit preparation effort

Procurement Paths

- GSA MAS for IaC engineering and automation services
- DoD ESI for GitLab and infrastructure tooling
- NASA SEWP V and SEWP VI for automation platform licensing

Compare vehicles and ordering steps on **How to buy**.

Partner Technology Examples

- Red Hat (Ansible)
- GitLab
- Spectro Cloud
- VMware

This is a representative use case. To request a briefing or a quote, contact Norseman Defense Technologies at 410.579.8600 or sales@norseman.com.