Continuous compliance & reporting

Connect repeatable policy checks, corrective processes, and evidence that operations, security, and compliance teams can review.

The business requirement

Network controls need to hold between formal audits as configurations and devices change. Collecting evidence by hand turns every assessment into another project. Gluware connects recurring assessment and reporting to the process used to correct failures.



HOW THE CAPABILITY WORKS

Define and evaluate controls

Config Drift & Audit owns audit policies and evaluates captured configuration or operational command results. The policy rules determine exactly which controls are checked.

Correct the failure

Config Model Editor provisions modeled CLI/API configuration changes. Network RPA coordinates the corrective tasks and any required external process. Reporting itself does not change the device.

Produce useful evidence

Config Drift & Audit exports detailed audit execution results. Data Explorer formats stored fields into reusable reports that can be viewed, downloaded, emailed, or scheduled.

Repeat and review

Run checks on demand, on a schedule with email notification, from syslog events, or through Network RPA workflows. Review integrated logs and reports. Git integration synchronizes and backs up/restores audit policies; Version Control can retain supported construct history.

Continuous compliance & reporting

Connect the operating process to defined component responsibilities.

COMPONENTS DELIVERING THE CAPABILITY

Config Drift & Audit	Owns policy evaluation and detailed audit exports.
Data Explorer	Builds reusable reports from stored fields.
Config Model Editor	Performs modeled CLI/API corrective changes and CLI/API state assessments.
Network RPA	Coordinates checks, corrective tasks, and reassessment.
Dashboard	Presents operational status and context.
Version Control	Provides supported audit-policy and construct history.

OPERATING SCOPE

Config Drift & Audit: evidence and correction

Integrated logging and reporting support investigation and evidence. Network RPA can connect findings to corrective tasks; Config Model Editor performs modeled configuration changes and separate node state assessments.

Data Explorer: reporting

View report results and history, download reports, or email them to the people who need them. The underlying applications supply the data being reported.

Network RPA: process coordination

Connect targets, tasks, variables, conditions, scheduling, triggers, and notifications across Gluware applications and external systems. Each task uses its supported application or execution mechanism.

Business value and measurement

The outcome is sustained control over the requirements covered by the checks, with evidence available for review. Measure recurring failures, time to resolution, coverage, and exceptions. The organization determines the regulatory requirements and broader evidence it needs. Ongoing compliance uses scheduled or triggered assessment, rather than assuming uninterrupted streaming evaluation.

Technical documentation | Request a demo