IP FABRIC

Use Compliance Automation to meet Regulatory Obligations and Strengthen Operational Resilience

Automated network assurance paves your way to continuous compliance and proactive audit readiness

ipfabric.io

Compliance Requires a Complete Understanding of Your Network?

Compliance regulations and the frameworks, controls, and requirements that accompany them offer a blueprint for operational stability and security that is critical to protect your business and your customers. Compliance frameworks cover the foundation of any digitally dependent business: the IT network, cloud, and security architecture.

Digital operational resilience is a prerequisite for successful compliance - and an outcome of striving for it. Likewise, compliance programs are a catalyst for risk reduction and help ensure the availability of critical services, which is the ultimate purpose of regulation. Your network and cloud infrastructure state are a lynchpin of compliance.

Following compliance blueprints and meeting compliance reporting requirements, however, is impossible when you know that you don't have the necessary insight into your infrastructure:

- **Assets – every switch, router, firewall, and load-balancing device in your network.**
- **Interdependencies – the relationship between these assets.**
- **Traffic Flows – specific routes from network ingress to egress, and everything a data packet touches on the way.**

These end-to-end insights help you map critical services onto your network and cloud instances and understand where and how the resilience of critical services depends on your network or cloud assets, topology, and policy.

Why Actionable Proof of Compliance Is So Critical

Regulatory requirements are not necessarily strictly prescriptive as to how you achieve this operationally resilient state, but they all require proof of your processes, people, and technology that underlie your compliance program.

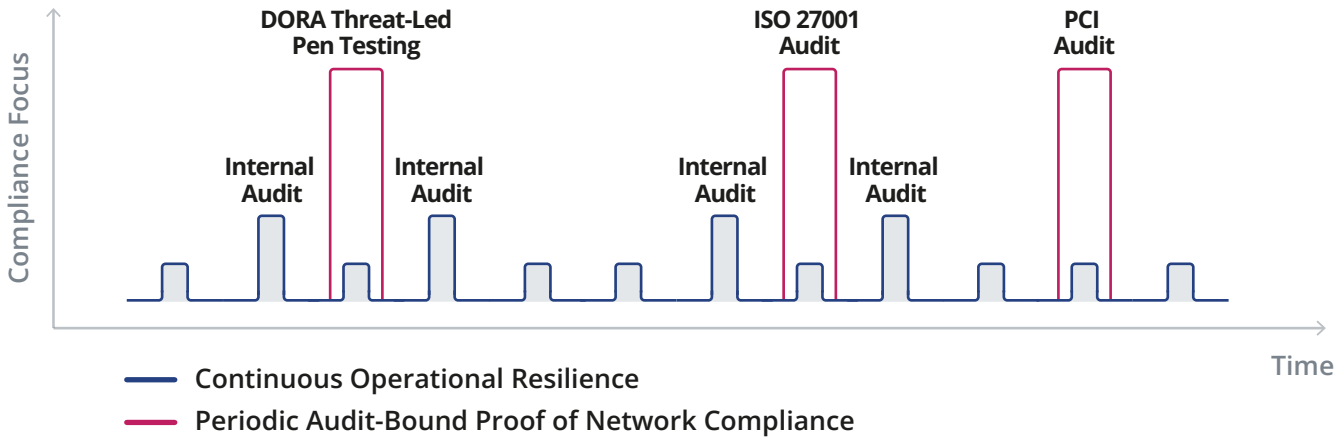
Producing the necessary documentation for an audit can feel like another burden thrust upon the network teams' ever-growing responsibilities. However, having this evidence at audit time - and all the time - drives stability, security, and business acceleration.

When you have an easy way to document assets, interdependencies, and traffic flows on a daily basis, everyone from the Board of directors to individual engineering benefit:

- **The Board can trust their C-suite to protect the business reputation and mitigate operational risk;**
- **C-suite can empower technology leaders to move transformative initiatives forward safely;**
- **The digital business is more reliable and secure, as the MTTR of incidents is reduced, configurations are more compliant, and there are fewer unexpected vulnerabilities to impact network stability and security and;**
- **Team members no longer need to manually generate documentation and have time to work on exciting projects.**

The Burden of Proving Compliance

There are two compliance reporting requirements that network teams need to be ready for at any moment: (1) Continuous Operational Resilience and (2) Periodic Audit-Bound Proof of Compliance for every regulatory compliance framework that applies to the organization. Compliance audit preparation and reporting never ends. Here's an example of how the workload might look like in a financial institution for just three regulatory frameworks:



Network Assurance Platforms Make Digital Operations More Stable and Secure

The IP Fabric automated network assurance platform is essential to operational resilience and compliance reporting. How does IP Fabric offer the oversight needed for continuous operational resilience?

- **Holistic Network Governance:**
  Comprehensive but light-touch network discovery of the whole estate – vendor-neutral, cloud, and on-prem – means an accurate understanding of everything in your network, exposing previously unmanaged, unmonitored, or rogue network devices. Don't fall victim to shadow IT or legacy environment oversights.

- **Alerts and automation when deviation from intended compliance posture is detected:**
  Built-in and custom intent checks will alert your team or kick off an automated action in other platforms when inconsistent device configuration is detected. This allows for proactive remediation before it becomes a problem.

- **Quick Troubleshooting:**
  Automate the inclusion of root cause analysis information into trouble tickets for fast incident resolution.

- **Track EoL and EoS dates:**
  Leave behind fragmented network planning, with automated network inventory including essential information you'd otherwise have to chase down manually and record in static documentation that quickly becomes outdated.

- **Identify and Harden Vulnerable Devices:**
  Ensure every device in your network (including previously unknown, unmanaged, or rogue devices) is secured according to policy and operates as expected.

- **Validate Security Posture:**
  Validate the effectiveness of secure network access for a Zero Trust approach, segmentation, security policy application, and enforcement points. Find rogue devices, traffic that is bypassing firewalls, open ports, etc.

- **Safe Change Management:**
  Validate operational state before and after planned changes to avoid unintended consequences and ensure stability through inevitable unplanned change.

Network Assurance Platforms Automate Compliance Reporting

It's not enough to know internally that your network meets compliance requirements; external auditors require proof. The time and resources required to manually document and present the evidence required for auditing bodies are enormous. Often, a huge part of compliance itself is having consistent records available, so the inability to quickly hand over a clear understanding of your network in the same format as previous audits estate speaks volumes to a regulatory body.

How can IP Fabric ensure you're always audit-ready?

- **Automated Network Inventory Management:**
  Automatic, daily network snapshots mean inventory, documentation, and network maps are always up to date. Your months-old, incomplete, static network documentation might as well not exist to an auditor who wants to know what your network looks like today.

- **Normalization of Diverse Network Data:**
  The eyes on your network aren't always expert. Even the most brilliant network engineer can't be a subject matter expert on every domain, technology, and vendor within your complex network ecosystem. Offering network data through clear, normalized, and user-friendly dashboards, maps, tables, and reports, and making these available via API means you don't have to spend days collating complex network information to suit specific users' interests or technical levels.

- **Flexible Network Snapshots:**
  Snapshots of your network can be full or partial; include everything or just the layers concerning the interested party; highlight specific end-to-end paths through the network; provide a birds-eye view or drill down into details. This flexibility means you can tailor exports of network information to the task at hand, without heavy hands-on network data processing.

- **Share Network Data Wherever It Needs to Go:**
  An open API and multitude of pre-built integrations enable sharing your proof of compliance easily with other teams or systems.

> **"It's not enough to know internally that your network meets compliance requirements; external auditors require proof.**

Generally speaking, regulatory compliance reporting requirements include records of:

Assets	Interdependencies	Traffic Flows
Discovery: Complete discovery of network assets to provide an inventory of knowns and unknowns. **Scope:** Establishing the boundaries of the network-identifying borders beyond which third parties, ISPS, etc manage adjacent infrastructure. **Lifecycle:** Show that you can determine when owned and managed assets are EOS, EOL, EOM. **Hardening:** Validate configuration standards are applied. **Vulnerabilities:** Demonstrate that you're checking against the NIST CVE database. **Backups:** Prove you're storing configuration backups for devices so they can be restored to new devices in case of failure.	**Map Topology:** Build a trust-worthy view of the network that changes with it. **Segmentation:** Validate the extent of network segments and policy enforcement between them.	**Record Critical Service Paths:** Show that you understand how services are dependent on network infrastructure client to workload. **Validation Of Business Continuity:** Show that services will continue to function after DR invocation.

IP Fabric Automated Network Assurance Platform for Compliance Automation and Digital Operational Resilience

IP Fabric offers an automated network assurance platform that delivers operational stability and security, which is the foundation for compliance, starting with vendor-neutral discovery and providing network proof needed to comply with various voluntary and law-bound compliance frameworks.

Beyond eliminating the bursts of manual efforts needed for specific audit dates, IP Fabric allows for continuous oversight of critical functions and enforcement of regulatory compliance and compliance with internal standards, protecting your network with daily snapshots that can be put to work to manage the ongoing changes that are a given in any complex enterprise network environment. The controls provided by IP Fabric apply to multiple regulations, saving you time and costly resources in preparing regulation-specific evidence. For example, let's look at what IP Fabric would provide for a Financial Services enterprise across several financial frameworks and regulations. Note that this example is indicative of some key overlap areas and is not comprehensive:

Compliance Automation	Compliance Regulation			
Network Assurance	**PCI**	**DORA**	**NIS 2**	**NIST CSF**
Assets Network Discovery Network Mapping Updated Inventory Low-level Design Documentation Network Analysis Report	Reqs. 12.3.4 12.5.1	**Identification** Article 8.1 Article 8.4 Article 8.4 Article 8.5	Cyber Risk Management, Corporate Responsibility, Reporting Duties Chapt. IV, Art. 20 Chapt. IV, Art. 23 Chapt. VII, Art. 32	**Identify** ID.AM-01 to ID.AM-08 **Govern** GV.RM-01 to GV.RM-03 **Protect** PR.PS-03
Interdependencies Flexible Topology Modeling Security Policy Validation Network Segmentation Validation De-risked change management	Reqs. 1.2.3 1.2.3.b	**Protection & Prevention** Article 9.2 **Response & Recovery** Article 11.5 **Reporting** Article 19	Cyber Risk Management, Business Continuity Chapter IV, Article 21	**Identify** ID.RA-01 ID.RA-02 ID.RA-03 ID.RA-05 **Protect** PR.IP-01 PR.AC-01 PR.AC-02 PR.AC-03 **Detect** DE.CM-01 DE.CM-07 DE.CM-08 **Respond** RS.MI-01 RS.MI-02 RS.MI-03
Traffic Flows End-to-end network path lookup Historical point-in-time network snapshots	Reqs. 1.2.3 1.2.3.b	**Protection & Prevention** Article 9.2 Article 9.4 **Response & Recovery** Article 11.4 **Backup & Restoration** Article 12 **Testing of ICT tools & systems** Article 25	Cyber Risk Management, Business Continuity Chapter IV, Article 21	**Identify** ID.AM-03 ID.AM-05 **Protect** PR.IP-10 **Detect** DE.CM-01 DE.CM-07 DE.CM-08

A similar framework can be applied to whichever set of compliance regulations you need to meet within your industry, geography, and size. You can only manage what you can measure, and IP Fabric offers a means to measure network behavior in relation to your ideal network state, and therefore, properly manage both daily network operations and long-term strategic initiatives.

About IP Fabric

IP Fabric is a vendor-neutral network assurance platform that automates the holistic discovery, verification, visualization, and documentation of large-scale enterprise networks, reducing the associated costs and required resources whilst improving security and efficiency.

It supports your engineering and operations teams, underpinning migration and transformation projects. IP Fabric will revolutionize how you approach network visibility and assurance, security assurance, automation, multi-cloud networking, and trouble resolution.

Don’t take our word for it

See how assurance can transform your approach to network management.

Access the demo

IP FABRIC

Support & Documentation
https://docs.ipfabric.io

HQ Office Boston
98 North Washington St.
Suite 407
Boston, MA 02114
United States

+1 617-821-3639

IP Fabric UK Ltd.
Gateley Legal,
1 Paternoster Square,
London,
England EC4M 7DX

+420 720 022 997

IP Fabric s.r.o.
Kateřinská 466/40
Praha 2 - Nové Město,
12000
Czech Republic

+420 720 022 997

ipfabric.io