SOLUTION OVERVIEW

Maintaining Governance, Risk, and Compliance and Streamlining the Audit Process

Straying from governance, risk, and compliance standards can be costly. Between August and October 2020, a bureau of the U.S. Department of the Treasury imposed $625 million in fines on major financial institutions.[1]

KEY BENEFITS

Detailed Visibility Into Audit Risk Vectors

Small problems can stay hidden until it's too late. And when that happens, your auditors have already imposed costly fines or assigned tedious proof-of-compliance work. By visualizing your applications as a whole, you can quickly find and isolate or resolve issues before they become bigger, no matter where the problem may hide.

Out of the Box, Compliance-Ready Solutions

Auditors expect a higher degree of cyber maturity from financial services institutions. Checking the compliance boxes is often not enough. F5 solutions are purpose-built to drive a high level of cyber maturity, impressing the auditors, and therefore minimizing the friction and stress caused by audits.

F5's Industry-Proven Support

F5's industry-proven support can guide you to create the critical standards and procedures required to best prepare your organization for audits of all types. We can also be by your side during auditor meetings to help drive compliance topics deeper.

You never know when the next audit is going to start. Once it does, you may lose the time and efforts of a full-time engineer for up to six months, who will have to do the necessary research and proof-of-compliance work.

Unfortunately, there are plenty of real-world instances where the OCC can fine organizations, as they recently did to a major U.S. bank in the amount of $85 million. In their findings they cited:

> *The bank has failed to implement and maintain an effective compliance risk management program and an effective information technology risk governance program commensurate with the bank's size, complexity and risk profile.*[2]

Staying within governance, risk, and compliance standards can be tough, but it shouldn't stop you from reaching critical business goals. With F5, you can streamline the audit process, and it starts with having mature cybersecurity.

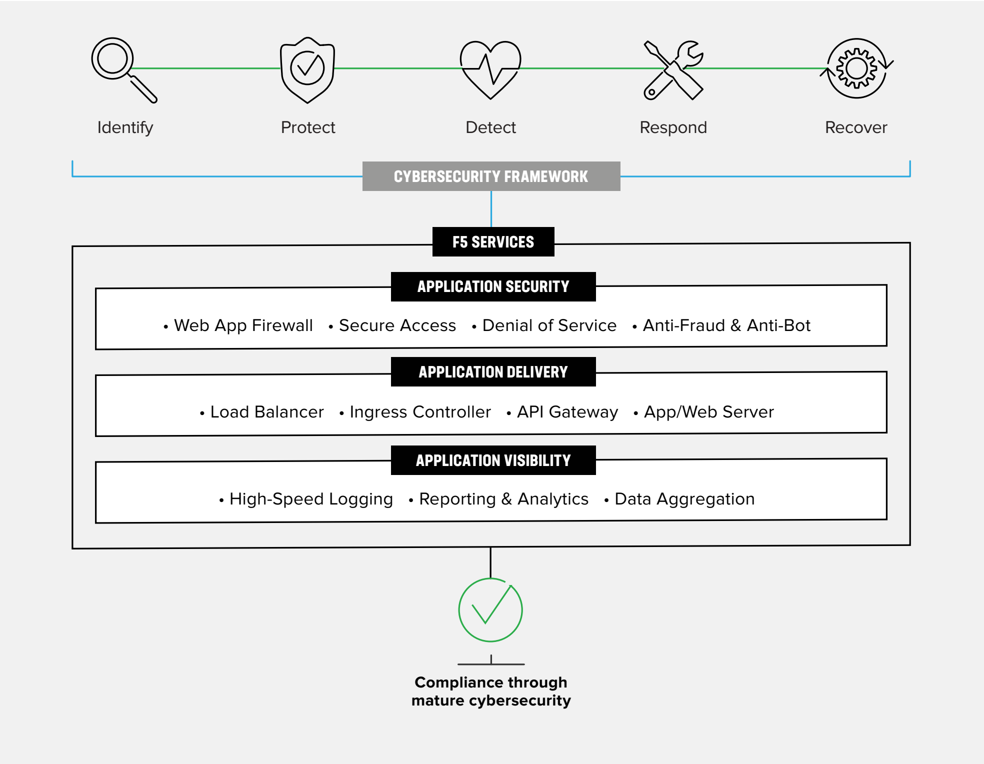

Identify
Protect
Detect
Respond
Recover
CYBERSECURITY FRAMEWORK
F5 SERVICES
APPLICATION SECURITY
• Web App Firewall • Secure Access • Denial of Service • Anti-Fraud & Anti-Bot
APPLICATION DELIVERY
• Load Balancer • Ingress Controller • API Gateway • App/Web Server
APPLICATION VISIBILITY
• High-Speed Logging • Reporting & Analytics • Data Aggregation
Compliance through
mature cybersecurity

Figure 1: This diagram highlights the critical components for achieving mature cybersecurity, a key ingredient in compliance.

Compliance Is More Than a Checkbox

To effectively streamline the audit process you need to be proactive. The right approach and app solutions are critical. F5 has a broad range of products and services that can help.

Product	How They Help
BIG-IP Access Policy Manager®	Access control, SSL VPN
BIG-IP Advanced Firewall Manager™	Firewall controls, segmentation, access
BIG-IP Application Security Manager™ Advanced WAF®	Application security, vulnerabilities (WAF is mandatory for PCI DSS compliance)
Beacon	Analytics and visibility insights into end-to-end application flows and infrastructure components
BIG-IQ® Centralized Management	Management platform, configuration management, telemetry, logging
Cloud Services	DNS, DNS Load Balancer, Essential App Protect—provide security controls, analytics, and visibility for regulators and auditors, experience and support.
BIG-IP DNS	DNS security (prone to attacks)
NGINX Controller™	NGINX Ingress Controller is a best-in-class traffic management solution for cloud-native apps in Kubernetes and containerized environments.
NGINX Plus®	Access, logging, WAF
Shape®	Fraud prevention, bot protection, deny/deceive options
Silverline®	SOCS, DDoS mitigation, application security, bot protection, configuration management (WAF is mandatory for PCI DSS compliance)
SSL Orchestrator®	Visibility, SSL decryption at scale
Secure Web Gateway	Web gateway, external access, data leakage

IN 2019, FROM THE TOTAL POPULATION OF ORGANIZATIONS ASSESSED ON PCI DSS COMPLIANCE, ONLY 27.9% OF ORGANIZATIONS ACHIEVED 100% COMPLIANCE DURING THEIR INTERIM COMPLIANCE VALIDATION.[3]

Creation and Governance of Standards and Procedures

F5's industry-proven experts can guide you to create the critical standards and procedures required to best prepare your organization for audits of all types. Without a hyper focus on compliance and ongoing vigilance, organizations can often fall short in critical regulations and compliance standards, like in Payment Card Industry Data Security Standard (PCI DSS) validation processes.

An Evolved Application Methodology Is Key

Trying to build and deliver modern, convenient applications using legacy infrastructure presents challenges and limitations, especially when considering compliance requirements. As institutions advance in their digital transformation, a flexible, extensible Enterprise Application Architecture (EAA) can help drive consistency and alignment to support outcomes at scale—a key requirement for meeting expectations around application security, performance, and reliability.

An evolved EAA approach aligns innovation efforts with business strategy and supports easy integration of emerging technologies to help organizations stay agile. With the right EAA in place, developers are better able to deliver modern applications swiftly and securely, regardless of location or device, and in compliance with standards and regulations.

Step 1: Align EAA and business goals, and determine the appropriate balance of innovation, agility, and risk.

Step 2: Take an application inventory. Account for all the applications in the enterprise portfolio.

Step 3: Assess the security risk for each application in the portfolio and assign the appropriate solution. Some examples include:

- FIPS certification of hardware and software as needed to meet standards and regulations
- Web app and API protection to guard against existing and emerging OWASP threats
- SSL orchestration with dynamic, policy-based decryption, encryption, and traffic steering through multiple inspection devices

Step 4: Define application categories and specify the application services required for each.

Step 5: Set parameters for application deployment and management. This includes:

- Understanding deployment options
- Evaluating associated costs, consumption models, and compliance/certification profiles

Step 6: Assign roles and responsibilities. You'll want to:

- Clarify who's responsible for each component within the EAA, including security.
- Recognize that responsibility may reside with individual contributors, departments, or cross-functional committees.

Step 7: Enforce the EAA approach throughout the organization to optimize security. This includes:

    - Leveraging automated mechanisms like user access controls or code vulnerability scans
    - Getting the organization on board through employee training and communications

Step 8: Work with F5 experts to ensure you are achieving continuous cyber maturity.

Critical Roles to Assign in Creating Governance of Standards and Procedures

CONFIGURATION COMPLIANCE TEAM LEAD

- Configuration management can be difficult to implement, which is why it’s imperative to designate a lead. Automation tools to help maintain configuration standards and minimize configuration drift include:
    - Declarative onboarding
    - AS3
    - Telemetry streaming
    - Cloud formation templates

ENTERPRISE APPLICATION ARCHITECTURE TEAM LEAD

- This critical function will lose its way without someone overseeing the progress and prioritization of this initiative. Organization-wide standards will also falter without this dedicated role.

AUDIT OWNER

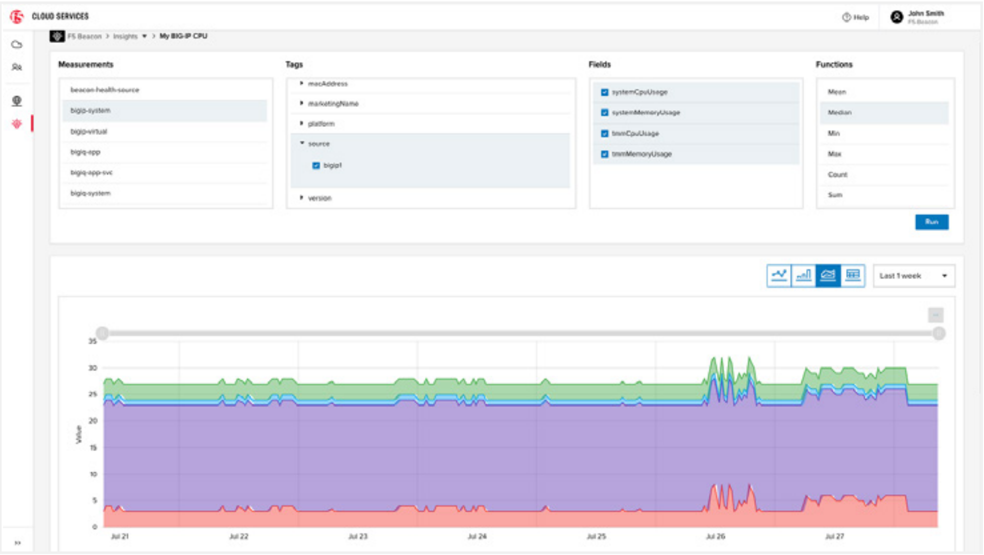
- Ongoing visibility around key audit topics is critical per audit. Each team needs a team lead that owns F5 solutions, and how they leverage deep data from the application and network to provide insights needed to quickly resolve audit-related problems.
    - Shared application-centric dashboards from F5 give your networking, dev, and security teams access to the data they need while supporting collaborative problem solving.

Streamline the Audit Process

When audits do happen, and they will at the worst times, F5 can be there to help you streamline the audit process. Our decades of experience; detailed analytics and telemetry; and out-of-the box, compliance-ready solutions were purpose-built to minimize the friction and stress caused by audits.

It all starts with detailed analytics. Check your applications' health status and security posture and use actionable insights from customizable dashboards to satisfy your many compliance inquiries–all in a simple, easy-to-consume SaaS model.

When your auditor makes a request, they can pull exactly what they're looking for within minutes.



Measurements
- beacon-health-source
- bigip-system
- bigip-virtual
- bigiq-app
- bigiq-app-svc
- bigiq-system

Tags
- macAddress
- marketingName
- platform
- source
  - ☑ bigip1
- version

Fields
- ☑ systemCpuUsage
- ☑ systemMemoryUsage
- ☑ tmmCpuUsage
- ☑ tmmMemoryUsage

Functions
- Mean
- Median
- Min
- Max
- Count
- Sum

Figure 2: Application details at a glance–quickly view your application-specific topology, health, insights, and event details.

With F5, you're not alone in the next audit process. Ask our experts to help drive compliance topics deeper, no matter what comes out of your next auditor meetings.

F5 can help:

- Uncover encrypted threats
- Deliver details around access controls to better manage privileged user access
- Customize exportable reporting to speak to specific audit requirements
- Provide cautions around security controls

Conclusion

Audit processes can be time consuming and stressful. Financial service employees never know when the next audit will start and the associated work often requires a full-time job, which is rarely funded. Without the right solutions and support in place, audits can last up to six months, leading to remediation work and another audit.

F5 has a proven track record in streamlining the audit process for financial services institutions. Our solutions are purpose-built to minimize the friction and stress caused by audits.

To learn more, explore F5 Banking and Financial Services solutions or contact your F5 representative.

[1] OCC and HIPAA Cybersecurity Regulator Fines Now in Hundreds of Millions, found at https://www.f5.com/labs/articles/cisotociso/occ-and-hipaa-cybersecurity-regulator-fines-now-in-hundreds-of-m

[2] OCC Report Finding, found at https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-135.html

[3] Verizon 2020 Payment Security Report https://www.verizon.com/business/resources/reports/payment-security-report/