Accelerating Financial Services Innovations

Leveraging Environment as a Service

Quali | Infrastructure Automation at Scale™

How to shift IT infrastructure security, certification, and compliance into high gear

Financial organizations are developing new financial services and business applications that require frequent modifications to their IT network infrastructure. These modifications are often driven by dynamic conditions pertaining to cybersecurity threats as well as compliance and certification requirements of financial regulations. The challenge facing IT departments when addressing these requirements is multi-faceted, ranging from legacy equipment, expensive test environments and the lack of automated tools to test and certify software updates.

This paper provides details on how to address these challenges by introducing the Quali CloudShell platform. An example will outline how IT departments can implement the Environment as a Service solutions to save weeks and months of certifying the security, compliance and certification requirements of IT infrastructure. As a result, IT departments will be in a position to enable and validate any infrastructure modification and support dynamic business needs.

Contents

Introduction

The ability to adapt quickly, have predictable revenue streams and meet new customer demands is based upon how quickly your organization can adapt to market and technology shifts. This is particularly true for financial services institutions (FSI), where time is literally money. Speed to market for financial service institutions depends on how quickly they can remove friction from customer engagement and leverage technology as a differentiator. Today, with every company becoming a technology company, and with financial institutions becoming software powerhouses, the introduction of new functionality for financial applications often requires software updates and cybersecurity enhancements to meet industry regulations. However, a seemingly "simple" update to their financial application such as a loan application on a borrower portal, whether it be in the data center or cloud, is never trivial. In fact, applying security & compliance policies and automating the modification of IT infrastructure easily becomes a multi-month long undertaking. FSIs are among the highest regulated industries and constrained to meet compliance requirements. With applications becoming distributed and accessible via different endpoints, test environment complexity becomes significant. One of the critical requirements during these stages is to ensure that the introduction of even minor changes meets industry certification standards without compromising on the speed of application rollout. The challenge before IT infrastructure and financial application teams is to accelerate this process without compromising on integrity.

> **Time is literally money.**

This paper will provide an example of a solution framework that the IT Network and Infrastructure teams can utilize to address financial services challenges with emphasis on:

- The impact that network updates have on security and compliance
- The impact of IT infrastructure updates on financial applications
- A strategy for efficiently introducing, testing, and validating IT infrastructure and application updates

The following illustration, Figure 1, depicts a high-level work flow that will be referenced throughout this paper. It highlights an end user accessing a financial application that is hosted on an organizations enterprise data center.

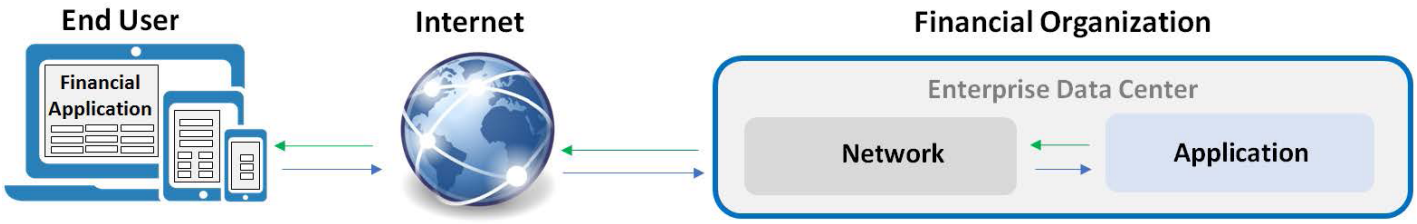


Figure 1: End user application communication workflow

1

IT Infrastructure Updates: Impact on Security & Compliance

IT infrastructure updates can be driven by multiple factors, i.e. new business initiatives in addition to security and compliance requirements. Security and compliance challenges can range from people and processes to location and solutions, with the IT infrastructure as the critical core for endpoint or application communication. The ownership of the products and services that comprise the IT infrastructure may include several cross-functional teams.

These teams may include network, server, storage, database, application, and extend to DevOps and SecOps groups. Team responsibilities include the facilitation of network communication as well as securing and protecting information derived from customers and partners.

Security

Cyber threats, whether introduced from internal bad actors or external malicious sources require dynamic protective measures to mitigate attacks that cause IT infrastructure or business applications to stop responding to legitimate requests. The attacks may introduce malicious script injections, denial of services as well as privileged escalations of credentials. In addition, internal bad actors can be identified and thwarted as they attempt to sabotage the enterprise data center and steal intellectual property. Security updates for IT infrastructure and applications are usually driven by advisories that are published by trusted governing bodies. The National Institute of Standards and Technology (NIST) and the Common Vulnerabilities & Exposures (CVE) are two examples. The challenge with these cybersecurity threat publications is the unknown and unpredictable behavior of the IT infrastructure and the financial application once the recommended updates have been applied. The IT and application teams may not be aware of the implications that a simple update may introduce across the network and application value chain. As an example, application security updates may introduce network port and protocol modifications that are not supported by the IT network infrastructure products. In addition, any third-party or external resource requests will also require verification and validation tests to ensure the cyber threats are addressed.

Compliance

Financial Services organizations are required to adhere to both geographic and industry specific regulations. Their enterprise data centers follow regulations such as ISO 27001 and Service Organization Control (SOC2) which require information and security management measures in place. Consumer financial protection measures are also in place via several compliance bodies that range from general customer rights to privacy requirements which ensure the security and confidentiality of customer records and information. The Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry Data Security Standards (PCI DSS) in the United States are two examples of regulations that require adherence. For example, GLBA provides guidelines on how to comply with the safeguard rules by ensuring a security & compliance plan is in place to protect customer information (GLBA Guidelines). In addition, Financial Services organizations may have monthly or annual audits which will include international information residency requirements as outlined in the EU-US Privacy Shield (which replaced the International Safe Harbor laws) and PIPEDA in Canada.

Quali

Figure 2: Financial Services Compliance Advisory Organizations and Frameworks

Together, both cybersecurity and compliance regulations require immediate attention in order to assess the business application and IT infrastructure implications. Cybersecurity vulnerabilities may require the organization to accelerate software updates that have not had the opportunity to be fully tested and validated for deployment. This can introduce business risk by compromising the IT infrastructure.

2

IT Infrastructure: Network Component Updates

Security and Compliance requirements may be driven by a variety of factors that necessitate an update for one or more of the IT infrastructure components. These factors may include real time cybersecurity threats published by governing agencies or results from an internal audit. In addition, security penetration tests may also be included to determine the risk posture of an organization.

Once the factors have been identified, a determination can be made regarding the infrastructure components requiring modification. These modifications fall into one of two categories that are identified as either a firmware or a configuration update. Firmware updates are primarily related to forecasted releases based upon a pre-determined roadmap and software release schedule. Configuration updates can vary from modifications in IT policy to security related issues that require changes due to industry specific regulations.

Products associated with a security or compliance update:

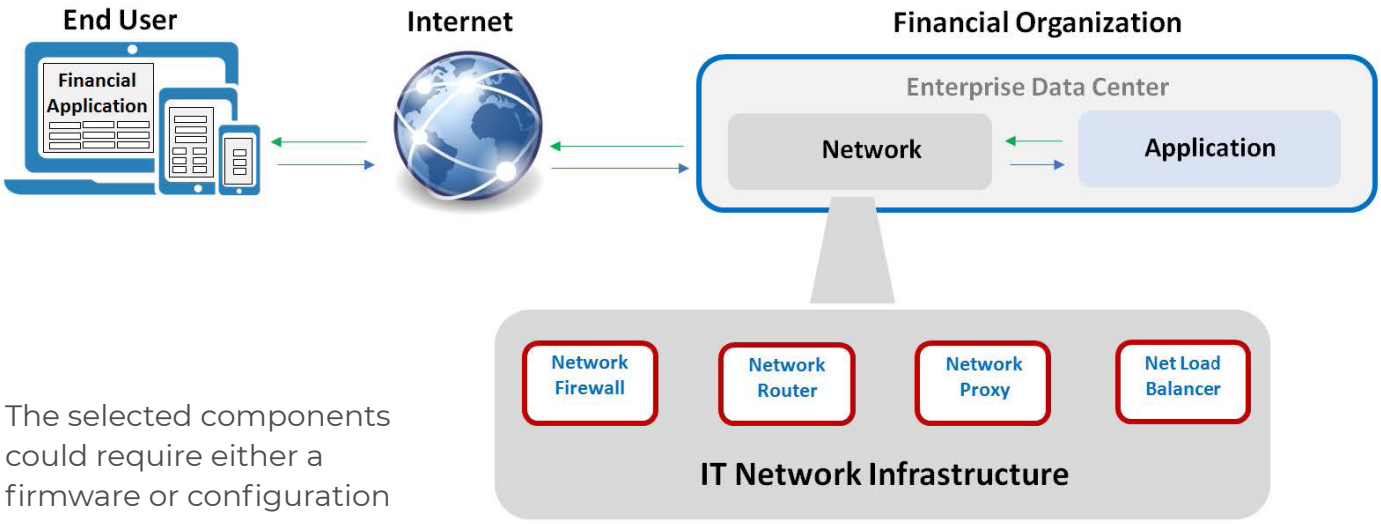


Figure 3: IT Network Infrastructure Components

The selected components could require either a firmware or configuration update, or in some cases both. This often occurs where scheduled updates were going to take place and an opportunity to modify the configuration can also be implemented. An example of the software update requirements are provided in Figure 4.

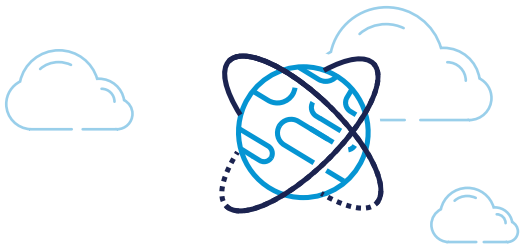
Enterprise Data Center	IT Network Infrastructure			
	Firewall	Router	Proxy	Netload Balancer
Firmware Update		15.4 ▸ **15.5**	6.5 ▸ **6.6**	
Configuration Update	7.0 ▸ **8.0**			11.0 ▸ **12.0**

Figure 4: IT Network Infrastructure Update Requirements

Interoperability mapping between the various infrastructure technologies is crucial as components get upgraded or patched. For example, an update on a network router may also necessitate an update on the next hop devices that are in the communication path.

3

IT Infrastructure: Technologies



The transportation and distribution of information across the IT infrastructure core can include an array of technologies. These technologies can range from traditional vendor centric hardware solutions to Software-Defined Networking (SDN), Network Function Virtualization (NFV), Application Delivery Controllers, and Hyper-Converged solutions. A sample of IT infrastructure components are listed below:

Proxies

Routers **Switches** **IDS/IPS**

SDN/NFV **Hyper-Converged** **Firewalls**

Wireless **Application Delivery Controllers**

Security Gateways **Load Balancers**

For illustration purposes, we have selected a subset of the aforementioned components and mapped them to specific products to demonstrate how the end user client requests are serviced through the IT network infrastructure tier:

Enterprise Data Center	IT Network Infrastructure			
	Firewall	Router	Proxy	Netload Balancer
Firmware Update		15.4 ▸ **15.5**	6.5 ▸ **6.6**	
Configuration Update	7.0 ▸ **8.0**			11.0 ▸ **12.0**

Figure 5: IT Network Infrastructure Update Requirements

The end user client, public internet, and the selected IT network infrastructure components are detailed in Figure 5. The infrastructure vendor components may vary by organization due to other variables i.e. cost, form factor, open source software, proprietary software, etc.

Customer web browser interface for the financial application

Cisco routers to support traffic dissemination between network segments

Public internet domain that redirects client requests to the origin or application server

Bluecoat/Symantec proxies to support forward and reverse proxy rules

Palo Alto Networks Firewall for security policy enforcement

F5 Network hardware load balancers to efficiently manage customer requests

Figure 6: Information Workflow Elements and Components

4

IT Network Infrastructure: Test Workflow

The introduction of firmware and security related configuration updates requires a validation process to ensure that the updates were effective. A majority of the organizations have a methodology that describes the validation process so that it is repeatable across each line of business. Nevertheless, the challenge with testing the updates is one of following a methodology and ensuring the required resources are available as described.

Methodology

Each organization may have an IT Service model that they utilize for standard software deployments. Several methodologies exist that include Information Technology Service Management ISO 20000 or Information Technology Infrastructure Library. Typically, most of the service management methodologies follow a similar process as outlined below in Figure 6:

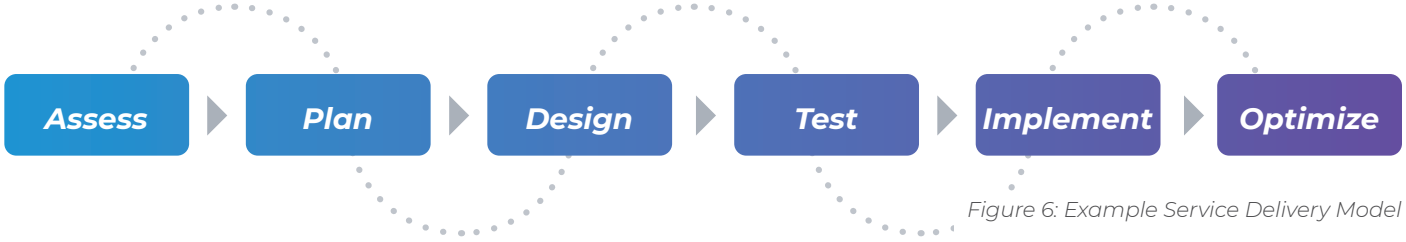


Figure 6: Example Service Delivery Model

People

Collaboration is required amongst multiple teams and subject matter experts. The project owner will require teams of IT Operations, Quality Assurance (QA), Security Operations (SecOps), and Development Operations (DevOps). New financial application development associated with IT infrastructure updates may also require application development teams. Increasingly, legal and privacy teams are involved if compliance dependent updates are required.

Tools

The test tools often vary between each department and line of business. For example, an open source software scan, load generation, or security scan tools provide different functionality based upon the selected vendor. Security and Compliance auditors rely on recommendations from technology and industry governing bodies that create the standards, rules, and regulations to determine which tools meet the requirements.

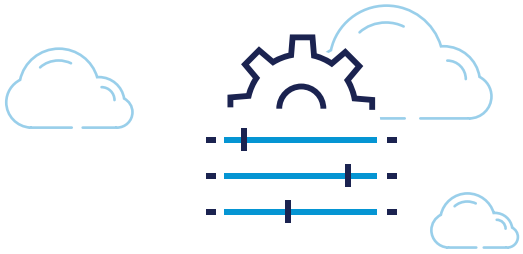
Time

Availability of the aforementioned teams is one of the inhibitors to completing the updates by a project due date. These teams have production related responsibilities and additional tasks are often outsourced to partner organizations that provide lab services. External resource requirements may extend the timetable due to validating, authorizing, training, and onboarding partner resources. Invariably, these activities extend the project timeline by weeks, if not months.

Budget

The most overlooked component for software update requirements is the amount of financial investment required. Traditional budgetary approaches that were effective for legacy IT network infrastructure components may not be sufficient to combat the unpredictable cybersecurity threats and compliance requirements. New investments in streamlining test workflows and automating the test environment are replacing the legacy models which were heavily reliant on manual, non-repeatable tasks. The cost savings are substantial as infrastructure updates are sped up from weeks to days.

5



IT Network Infrastructure: Sandbox environments as automated test environments

Organizations that utilize an IT service methodology are able to allocate resources in a prescriptive manner for their infrastructure update requirements. The introduction of a sandbox environment enables the project team to gauge the success at each critical juncture of the test cycle. The sandbox environment can ensure that the infrastructure update requirements are correctly tested, validated and certified for any additional test criteria.

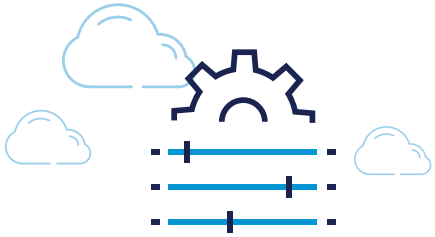
The sandbox environment is a dedicated test environment containing the IT infrastructure technology components, test tools, and solution architecture required for the test cycle. Each sandbox may have different owners and operate test scripts that are mutually exclusive for their requirements. The set-up and maintenance of both the sandboxes and test scripts can be very complex and time-consuming. Although automation is in place for repetitive tasks, a majority of the activity still depends upon manual processes. The following is a description of the most commonly utilized sandbox environments and naming conventions:

Dev/Test The Development and Test environment can take multiple forms. The sandbox environment may run on a developer's host machine or within a dedicated lab environment. The location is dependent on the infrastructure component that is being updated. Within a lab environment, the initial battery of tests are conducted by the IT Operations team responsible for the given infrastructure component. The team can consist of cross-functional subject matter experts for each of the required infrastructure components.

Quality Assurance (QA) The QA test cycle may require several environments to complete this phase of testing. There may be dedicated environments for functional unit tests, integrated solution tests, load, and performance tests. Due to the variety of test requirements, the QA team can have multiple team members specializing in specific infrastructure components, and experts who develop scripts and automated test tools.

Security Operations The SecOps environment allows for cybersecurity vulnerability testing ranging from surface scans to deeper component penetration tests. Test scripts can be automated to introduce cyber-attacks based on various threat criteria that pertain to identity, privileges, component accessibility, denial of service, or other attacks. Compliance templates and test scripts can also be introduced into this environment to validate adherence to regulations. Third-party scan and threat generation tools are often required to augment internal test tools.

Staging/Pre-Production This environment can be considered as pre-production and should mirror the production architecture as much as possible. Complete end-to-end solution tests are conducted with high availability and failover testing to determine infrastructure behavior during power or network outages. The team can include ITOps and DevOps or additional QA & SecOps folks as required.



Solution Test Sandbox Environment	Firewall	Router	Proxy	Netload Balancer
1: Dev Test/Lab				
2: Quality Assurance			Pass	
3: Security Operations				
4: Staging/Preproduction				

Figure 7:: Example of the four solution test sandboxes with pass or fail grade

6

Quali Environment as a Service: Automate and Streamline Test Workflows

Financial institutions can address the challenge of applying component updates in an efficient and timely manner by utilizing Quali's CloudShell solution. Quali's Environment as a Service solutions allow you to create and publish sandboxes that are replicas of infrastructure and application configurations and use them for development, testing, demos, training and support. The CloudShell platform helps you create self-service, on-demand environments that cut cloud costs, optimize infrastructure utilization, and increase productivity.

Summing Up:

IT departments are under tremendous pressure to ensure that their IT infrastructure can support new business requirements and continue to meet security and compliance demands.

These requirements are time sensitive and require expeditious software updates for the multitude of IT infrastructure components. The challenge is that IT departments lack flexible, efficient solutions that can quickly provision their infrastructure to support the financial business applications.

What is Quali?

Quali provides the leading platform for Infrastructure Automation at Scale. Global 2000 enterprises and innovators everywhere rely on Quali's award-winning CloudShell platform to create self-service, on-demand automation solutions that increase engineering productivity, cut cloud costs, and optimize infrastructure utilization.

Quali | Infrastructure Automation at Scale™

quali.com | info@quali.com

Information in this document is accurate as of 12/2/2020. Information may have changed after this date.

120220_v1