FCI

LEGACY IT MIGRATION

FIRM SECURITY

Reducing cost and increasing security by replacing legacy IT.

Over the past decade, financial services firms have moved away from legacy on-premise and virtual desktop infrastructure toward modern, cloud-first alternatives — and FCI has been helping them make that transition.

10+
years of successful migrations

100%
data preserved during transition

Zero
downtime for end users

THE LEGACY PROBLEM

Three solutions that made sense once — but no longer do.

For years, IT providers sold financial services firms on infrastructure that was expensive to maintain, difficult to secure, and impossible to scale. Local file servers, remote desktop access, and virtual desktop infrastructure were presented as reliable, proven solutions. In many cases, firms were told these approaches were more secure than the alternatives.

We know now that none of that was true. Legacy systems carry elevated risk, higher cost, and growing compliance exposure — often managed by local IT firms that wouldn't survive a vendor due diligence review. FCI has spent the last decade helping firms replace all three with modern, cloud-first solutions that are simpler to manage, easier to audit, and far more secure.

Local Servers | Remote Desktops | VDI

LOCAL SERVERS

Your file server doesn't belong in your office.

A local file server is a physical machine sitting inside the firm's office, storing critical business data — client records, financial documents, compliance files. For a long time, this was the standard. IT providers installed the hardware, configured the backups, and told the firm their data was safe.

The reality is different. An office cannot match the physical controls, redundancy, and monitoring of a professional data center. Patching, backups, hardware lifecycle management, and disaster recovery all fall on the firm or its IT provider — and in practice, these are often neglected until something breaks. A server with critical client data sitting behind a basic office firewall is a high-value target with low-grade protection.

Compounding the risk, access was routinely granted to outside IT firms through open firewall ports — vendors that were never subjected to a formal due diligence review as required under financial services cybersecurity regulations. When pressed on their security practices, the typical response was simple reassurance: "You can trust me." But trust is not a control. If that IT firm — operating without proper security protocols — gets compromised, the attacker inherits their access. That open port becomes an open door straight to your file server, your client data, and your regulatory exposure.

The cost is significant as well. Hardware needs to be purchased, maintained, and eventually replaced. Backup infrastructure has to be managed separately. When something fails, the firm is waiting on a technician to physically visit the office. None of this scales, and none of it needs to exist anymore.

> "The industry told firms their data was safer in their own office. It wasn't — and we've been helping firms fix that for over a decade."

THE MIGRATION PATH

From local server to Microsoft 365 SharePoint.

SharePoint is the firm's file server — hosted by Microsoft, protected by enterprise-grade security, automatically versioned, and stored across geo-redundant data centers. OneDrive is the client application that users interact with on their computers: it syncs files seamlessly, so the experience feels the same as working with local files. The difference is that the data is no longer in the office — it's in a data center with the kind of protection no office can provide.

SharePoint delivers advanced rights management, granular access controls, and a modern collaboration experience that a traditional file server simply cannot match — all while being easier to manage and significantly more secure by default.

FROM

Local File Server

Physical hardware in the office. Manual backups. Single point of failure. Hardware lifecycle and disaster recovery managed by the firm or its IT provider. And to allow remote access or vendor support, firewall ports must be opened to the outside — introducing exactly the kind of external exposure that regulators and attackers alike are paying attention to.

TO

Microsoft 365 SharePoint

Enterprise-grade security. Automatic versioning. Geo-redundant storage. OneDrive syncs files to each user's computer seamlessly — same workflow, better protection. And users no longer need to connect to the office at all; with an always-on Gateway VPN, they connect securely from anywhere, with every communication protected end to end.

REMOTE DESKTOPS

Opening the firewall was never a good idea.

When firms needed to give employees access to their office computers from home, the most common approach was remote desktop access — typically using RDP (Remote Desktop Protocol). The IT provider would open ports on the firm's firewall so users could connect from outside the network and control their office computer remotely.

This was always a security risk, and it has only gotten worse. Attackers actively scan the internet for open RDP ports. It is one of the most exploited entry points in cybersecurity — a known, well-documented attack vector that continues to be used successfully against firms that haven't closed those ports.

The other problem is what users were connecting from. In many cases, the device used to access the office computer was a personal laptop or home computer — unmanaged, unmonitored, and completely outside the firm's control. The promise was that it didn't matter what device the user had, because the work was happening on the office machine. That promise was false, and the regulations are clear on this point. Most were not using MFA to authenticate that connection either — a basic requirement that regulators have made explicit, and that most firms running these setups quietly ignored.

> THE QUESTIONS REGULATORS ASK
>
> *If an employee accesses client data from a personal device, can you demonstrate that the device meets your firm's security requirements? And if that device is lost or stolen, can you lock it down remotely? Regulators don't just want your policies — they want proof. Every device touching client data should be enrolled, inventoried, and managed, so you can demonstrate your cyber posture and act immediately when something goes wrong.*

VIRTUAL DESKTOP INFRASTRUCTURE

VDI solved one problem and created two more.

Virtual Desktop Infrastructure — VDI — was the next evolution. Instead of keeping the desktop computer inside the office, the IT provider moved it to a cloud data center. Users would connect to their virtual desktop from any device, and all the work happened in the data center rather than on the local machine.

On paper, this addressed the physical security problem of having a computer sitting in an office. But it introduced two new issues that firms are still dealing with today.

The first is cost. With VDI, the firm is paying for two computers: the virtual desktop running in the data center, and the physical device the user needs to access it. Licensing, hosting, maintenance, and support add up quickly — and the firm is essentially doubling its infrastructure without doubling its capability.

The second is the same false promise that remote desktops carried: you don't need to secure the end device. The idea was that since all the data lived in the virtual desktop, the physical device was just a window — a dumb terminal that didn't need protection. That was never true, and regulatory expectations have made it explicit. Any device used to access private data — regardless of where that data is stored or processed — must be protected, managed, and accounted for.

BAD USER EXPERIENCE

Users complain about it constantly — video calls stutter, lag, and drop. Worse, VDI often cannot support the software updates that cybersecurity regulations require, leaving firms stuck between operational limitations and compliance obligations.

FALSE SECURITY

The claim that the endpoint doesn't matter was never supported by the regulations — and it never reflected the actual risk.

COMPLEXITY

VDI environments require specialized management, licensing, and support. Troubleshooting is slower and more expensive than a well-managed endpoint.

UNMANAGED ENDPOINTS

Users often connect from personal or shared devices that sit outside the firm's security controls and asset inventory entirely.

REGULATORY REALITY

Every device that touches client data must be accounted for.

Whether the firm uses a local server, remote desktops, VDI, or modern cloud-first tools — the regulatory requirement is the same. Every device that stores or accesses private client data must meet a clear set of standards. This is not optional, and it applies regardless of how the firm's infrastructure is architected.

The false promise of remote desktops and VDI was that the endpoint didn't need to be secured because the work was happening somewhere else. Regulators have never agreed with that position. Any device used in the course of business — whether it's a firm-issued laptop or a personal computer connecting to a virtual desktop — must be protected, secure, compliant, and controllable.

01 **Protected**
Endpoint protection, encryption, and threat detection must be active on every device that accesses firm systems or client data.

02 **Secure**
The device must meet the firm's security baseline before it is allowed to access any system. This includes operating system updates, security configurations, and access controls.

03 **Compliant**
The firm must be able to demonstrate compliance at any time — not just during scheduled audits. Continuous compliance reporting is the expectation, not a one-time exercise.

04 **Controllable**
If a device is lost or stolen, the firm must be able to remotely wipe or lock it immediately. If this capability doesn't exist, the firm has a compliance gap.

05 **Inventoried**
Every device must appear in the firm's asset inventory with its current status and compliance posture. A device that isn't tracked is a device the firm can't account for.

> "If you can't show that a device is protected, secure, compliant, controllable, and in your inventory — then from a regulatory perspective, that device shouldn't be touching client data."

WHAT FCI DOES

FCI replaces legacy infrastructure with secure, compliant, cloud-first solutions.

FCI doesn't just remove the old infrastructure — we implement the controls and produce the evidence that the firm's cybersecurity program requires. The transition is planned, executed, and documented so the firm can demonstrate to regulators and home offices exactly what changed and why.

For file servers, FCI migrates the firm to Microsoft 365 SharePoint with OneDrive synchronization. Every file is preserved, every permission is mapped, and every user is trained on the new workflow. The firm's data moves from a single machine in an office to a geo-redundant, enterprise-secured cloud environment — without any downtime for end users.

For remote desktops and VDI, FCI transitions the firm to managed endpoints — secure, compliant firm-owned or BYOD computers that are controlled by the firm and protected by FCI's managed cybersecurity services. Users work directly on their own device with all the security, compliance, and monitoring built in. There is no second computer to pay for, no virtual desktop to maintain, and no open firewall port to worry about.

Every device FCI manages appears in the firm's asset inventory, reports its compliance status continuously, and can be remotely wiped or locked in the event of loss or theft. That is the standard the regulations require, and it is the standard FCI delivers.

> WHAT FIRMS OFTEN ASK
>
> *What happens to our files during the migration? Will users lose access? How long does it take?*

FCI's migration process is designed for zero data loss and zero downtime. Files are migrated incrementally, permissions are preserved, and users are transitioned in groups so the firm never loses access to its data. Depending on the file directory size and the current and planned configuration, most migrations are completed within a few months — and FCI handles the entire process end to end.

Ready to retire legacy infrastructure?

FCI works with broker-dealers & branch offices, insurance carriers & agencies, and RIAs. If your firm is still running on local legacy servers, remote desktops, or VDI — we can help you transition to something modern and better.

PHONE

973-227-8878

WEB

fcicyber.com