Collabrance Co-Managed IT Support: **Frequently Asked Questions**

What is co-managed IT?

Co-managed IT is a "hybrid" model of outsourced IT. We work with your existing internal IT team to identify the everyday support issues that can be managed by the Collabrance service desk, so your in-house team's time is freed to tackle higher-impact work. It's called "co-managed", because that's what it is: IT support managed through the cooperation of two technical teams – yours and ours.

How can Collabrance help my internal IT department?

Co-managed IT support can benefit your internal operations in a number of ways. The most impactful advantages include:

1. Save time
Co-managed IT support does not replace your in-house technical team – rather, we enhance the capabilities of your internal team by providing support where it's needed. The Collabrance co-managed IT offering focuses specifically on tier 1 issues, which account for 50% of support tickets, on average. That means 50% of support requests can be resolved without action needed from your team.

2. Save money
An investment in co-managed IT services means your company has access to and can leverage a team of highly trained, expert technicians, without the overhead of salary, benefits, and other long-term costs required to retain a full-time employee.

3. Scale up and down with ease
Collabrance co-managed IT support is priced on a flexible, per-user basis. That means we can adjust our support to align with your business as it changes over time, without personnel changes to your internal team.

What support issues can Collabrance manage for my internal IT department?

Our co-managed IT solution is similar to our Basic User Support offering, which provides live-answer user support for line-of-business and productivity application assistance, including:

- User support for MS Windows workstations – Office 365, password resets, mailbox changes, distribution lists
- Mobile devices and email connectivity
- Account unlocks
- Basic hardware troubleshooting
- Reboots
- Printer issues

If necessary, we can manage more specific user issues. Our team will provide a solution tailored to your unique business needs.

What does co-managed IT support look like for my company's employees?

In a typical co-managed environment, your employees would contact the Collabrance service desk directly for support requests – via live-answer phone, email, or desktop chat. The receiving Collabrance technician will open a support ticket and begin troubleshooting the user's issue. Out-of-scope issues or issues that can't be resolved within agreed-upon SLAs would quickly be escalated to your internal IT team. Our most successful co-managed IT customers are transparent about their Collabrance partnership and train employees to follow the co-managed support resolution process.

How does Collabrance work with my company's technical tools?

We will work with your team to evaluate what tools you may have in place to give Collabrance remote workstation control needed for user support. If your company uses virtual technology, we may need a solution to access the virtual system. Generally, whatever tools are being used by your entry-level technicians for remote access to answer basic support requests is where we would first look to determine how we work with your tools.

How does Collabrance communicate with my internal IT team?

We will work with you during onboarding to identify the people on your team who can help with escalated issues and requests we're unable to resolve. Our teams will work together to define the escalation process to ensure we're helping users in the most efficient way. We aim to learn your team's processes and practices and act as a seamless extension of your team. We will establish a cadence for regular, scheduled status meetings with your team, to provide reporting, discuss any issues, and ensure ongoing alignment.

How does Collabrance address security concerns?

We understand IT security is critical in any vendor relationship. Collabrance follows a rigorous set of IT protocols and applies the most up-to-date industry best practices for security compliancy and control.

Collabrance will only have access to the information and systems necessary to manage the tasks you want us to focus on. As the customer, your company decides what access allowances Collabrance has, and you control any adjustments made to that level of access.

We will not have direct connectivity to your company network – no virtual private network (VPN) will be established. We will not have administrative access to your internal systems or data, including financial information or customer information.

Any Collabrance activity within your network is logged and can be audited at any time.

We maintain a documented incident response plan and are insured. We are also SOC 2 accredited.

A detailed outline of our security policies and practices can be found here: Collabrance Co-Managed IT Support for Financial Institutions: Security Policies & Practices

What does the Collabrance co-managed IT offering cost?

Collabrance co-managed IT support is $40 per user, per month. We offer flexible contract options, and the per-user count can be scaled up or down as your business needs evolve.

How do I know if my company is a good candidate for co-managed IT?

The Collabrance co-managed IT offering was designed specifically for banks and financial institutions. If you are a mid-sized financial institution and can answer YES to any of these questions, co-managed IT will benefit your organization.

Do day-to-day support tasks bog my technical team down, keeping us from working toward higher-impact goals?

Are there knowledge gaps within our team?

Are there technical tools that would be useful to us, but that we don't have access to or budget for?

Does time off for vacation or illness put a strain on the rest of the team?

Could our company benefit from faster response times for user support issues?

Is our company growing at a pace we struggle to keep up with?

Do we lack the facilities and physical space to expand our technical team?

To learn more, visit our website, read our blog, or download our security policies & practices.