How IT managed security services can empower your IT innovation

Are your IT managed security services doing enough to support your growth?

WIPFLI

Overview

It's likely that your financial institution is already partnered with an IT managed security services provider. However, if they're not elevating your cybersecurity or IT strategy, it may be time to consider a change.

Most service providers cater to multiple industries, meaning they lack specialization in financial institutions' unique operations and regulatory demands. By engaging IT managed security services with industry-specific support, you benefit from professionals who understand your technology needs and the challenges you may face during IT optimization.

Acting as a strategic partner, they help identify the solutions needed to improve workflows and enhance the customer experience. Additionally, they keep you informed about the latest cyberthreats and regulatory updates, helping ensure your operations remain secure and compliant.

When you switch or augment your current provider with one that has enhanced capability, they can help further your IT innovation with support for:

- Developing an effective IT strategy.
- Scaling your IT operations to your growth.
- Keeping your IT infrastructure secure.

© Wipfli

A better IT strategy

Effective IT managed security services providers can offer strategic guidance on all aspects of your IT infrastructure and take a proactive role in helping you identify ways to use technology to improve productivity and customer experience.

Your institution can look for providers capable of helping you develop strategies for:

1. Modernizing your operations

Impactful IT managed security services providers can offer valuable insights on the IT infrastructure you need to create a modern workplace environment.

A reliable provider can assist in updating your IT infrastructure by replacing outdated systems and supporting IT resource management. This includes replacing deprecated, end-of-life equipment to avoid security vulnerabilities.

They can also help you confidently adopt the latest solutions, such as cloud infrastructure and software as a service (SaaS) platforms.

While cloud migration and SaaS tools can make your operations more efficient, flexible and secure, they often leave you responsible for setting permissions and access control. Your provider should help you mitigate those risks by developing industry-appropriate security strategies for cloud services and integrating new solutions with your core banking system.

2. Adapting to changing customer expectations

Modern customers expect seamless digital experiences that provide easy access to services and information. Look for IT managed security services providers that can help your financial institution stay competitive by offering guidance on the technology you need to enhance customer experience, including strategies for:

- Integrating customer data and using dashboards to track critical customer metrics.
- Enabling omnichannel communication.
- Using customer data to identify opportunities for cross-selling services and increasing wallet share.

51% of respondents to Wipfli's recent financial institution survey reported that improving digital member engagement is one of their top priorities for **2024**, with **42%** also citing data analytics and AI.

© Wipfli

Wipfli's recent banking survey found that:

57% of banks report considering outsourcing IT.

42% of banks report considering outsourcing information security.

Scalability that matches your growth

As your organization grows, so do your IT needs.

For many institutions, establishing an in-house team for IT and security operations is neither cost-effective nor viable. Employing enough staff to provide the level of support your institution needs requires substantial resources. And attracting and retaining staff can be equally challenging, given the current labor shortages.

An IT managed security services provider can help augment your staff, but many providers operate as smaller organizations with their own limitations. That means that as your institution grows, they may not have the capability to scale with you.

You need a provider with the bench strength to support you as your cybersecurity needs and IT infrastructure evolve.

Outsourcing these positions with an effective provider gives you the necessary staff and infrastructure without the cost of hiring. They can also help guide your institution's data security at the executive level with fractional or virtual CISO services.

© Wipfli

Cybersecurity that meets your regulatory and organizational needs

Financial institutions have to address evolving cybersecurity and IT challenges as they innovate and face increasingly sophisticated cyberthreats. To adapt to changing cybersecurity risks, work with an IT managed security services provider who can help you navigate the following:

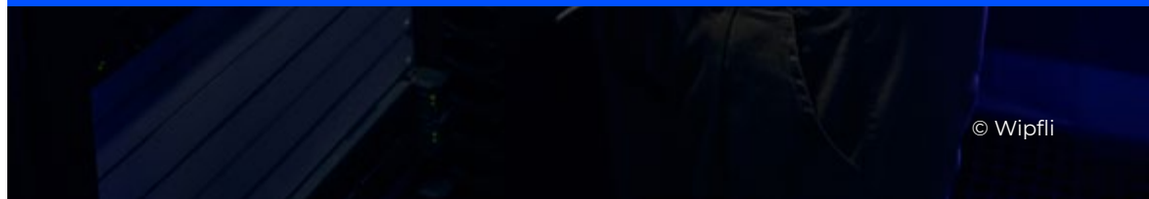
1. Regulatory priorities

Regulatory priorities on cybersecurity have shifted along with the threat landscape. Complying with the FFIEC Cybersecurity Assessment Tool — last updated in 2017 — may not be enough to protect your data and satisfy regulators.

Regulators are now focusing on new critical areas, including data recovery, access controls and operational resilience.

A capable provider is not only aware of these regulatory priorities but also able to assist you in updating your security controls to meet regulatory expectations.

Cybersecurity has become a growing challenge for financial institutions, with **43%** of respondents in **Wipfli's recent banking survey** listing it as one of their top concerns.



© Wipfli

2. Evolving cyberthreats

As cyberattacks become more frequent and sophisticated, you need an IT managed security services provider that can keep pace.

Effective providers work to improve your data protection while also adapting their own capabilities. An effective provider possesses the necessary tools, infrastructure and threat detection systems to swiftly identify indicators of compromise, such as advanced endpoint detection and response and AI-powered threat correlation.

Additionally, it's crucial to partner with a provider that maintains connections with various threat intelligence sources and knows the latest global threats, particularly those affecting financial institutions. Providers collaborating with organizations like FS-ISAC are better equipped to apply their knowledge of emerging threats to safeguard your institution.

3. Cyber resilience

Understanding how your organization will respond during and after a cyber incident is crucial to recovering from one successfully. Your IT managed security services provider should help you improve your cyber resilience with:

- **Data recovery testing:** Your IT services provider should assist with monthly file-level recovery tests and annual full recovery tests. They should work with you on recovery time objectives (RTO) and recovery point objectives (RPO) for critical functions and systems so that they understand their role in your plan and can help you with your business impact analysis.
- **Incident response:** Regularly rehearsing your incident response plan is essential for handling cyberattacks and business disruptions. Your IT managed security services provider should also be able to help you meet business continuity requirements and actively assist in preserving attack evidence.

© Wipfli

Take your IT managed security services further with Wipfli.

In a competitive and highly regulated industry, you need an IT managed security services provider who can do more than just help you meet regulatory compliance.

Wipfli's managed services combine industry specialization and proactive support, providing you with actionable recommendations for how you can enhance your cybersecurity operations and IT strategy.

With 24/7 monitoring and managed detection and response, we can help your institution stay ahead of the latest cyberthreats. And our IT road map service can help you navigate the technology you need to deliver a better digital experience.

We can also support your institution in areas including:

- Cloud security
- Data and analytics managed services
- Incident response and recovery
- IT health checks

Visit our site to learn more about how Wipfli can help you build a stronger cybersecurity program.

wipfli.com/fi

"Wipfli" is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP and Wipfli Advisory LLC (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services to its clients. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.