FINANCIAL SERVICES PLAYBOOK FOR PARTNERS: HOW TO TURN UNMET CLIENT NEEDS INTO RECURRING SERVICES

Delivered under your brand. Built for recurring services.

Use a current view of transaction systems, infrastructure, and third-party dependencies, paired with real-time insight into issues and impact, to help financial clients reduce risk, respond faster, and protect critical services.

www.wanaware.com

Version 1.1 — 2026

What's changing in financial infrastructure

Financial systems are faster—and more fragile—than ever.

They now depend on:

- Real-time payments
- Cloud and SaaS platforms
- AI-driven workflows
- Third-party providers across every layer

Everything is connected.

That makes it harder to answer:

- What systems are actually in use?
- What depends on what?
- What will break if something fails?

And when something goes wrong, it spreads quickly.

A small issue can turn into a major disruption.

What "assets" means in this playbook

In this context, assets include the systems and services that keep financial operations running, including:

- Core banking and payment systems
- Trading platforms and customer-facing applications
- Servers, cloud workloads, and APIs
- Third-party services and integrations

This is the infrastructure behind transactions, customer access, and day-to-day operations.

What financial clients expect now

Financial institutions are under constant pressure to:

- Protect transactions
- Maintain uptime
- Meet regulatory requirements
- Manage third-party risk

They expect partners to help answer:

- What systems and services are actually running?
- What is at risk right now?
- What depends on what?
- What will this change impact?
- What should we fix first?

The partner who can answer these becomes part of daily operations—not just incident support.

White-labeled for your practice

Your clients log into your portal, see your brand, and rely on your reporting. That lets you launch quickly and build a service they associate with your team—not another vendor.

Where partners get pulled in

Client situation	What the client asks	What is really going on
Security review	“Are we exposed?”	Unknown systems or connections
Audit or compliance	“Can we prove this?”	Incomplete or outdated records
System outage	“What failed?”	Dependencies unclear
Payment disruption	“Why did this happen?”	Hidden third-party dependency
Infrastructure change	“Will this break anything?”	Impact unknown
Performance issue	“Why is this slow?”	Root cause unclear
Vendor risk review	“What depends on this provider?”	No visibility into relationships

Why this is hard

- Systems change constantly
- Environments are highly interconnected
- Third-party dependencies are not visible

Hidden dependencies are what turn local issues into systemic failures.

These are the moments where partners step in—and where services can be built.

How partners can help — and why WanAware changes what they can do

Partners already help with:

- Audits
- Incidents
- Compliance
- Infrastructure planning

But today, answers are pieced together from:

- CMDBs
- Spreadsheets
- Monitoring tools
- Vendor systems

What WanAware changes

WanAware continuously discovers systems and maps how they connect.

Because observability is built on that real-time view of dependencies, you can:

- See what exists right now
- Understand how systems are connected
- Identify what is at risk
- Prioritize based on real impact

This replaces static lists with a continuously updated view of the environment

See how this works in practice:

- Learn more about Asset Inventory Management
- Learn more about Actionable Observability

When the client needs help with…	How it's done today	How WanAware changes it
Visibility into systems	CMDB + spreadsheets	Real-time inventory
Risk identification	Alerts and guesswork	Dependency-based prioritization
Incident response	Manual investigation	Root cause + impact clarity
Audit preparation	Manual reconciliation	Defensible records
Change management	Risky deployments	Predictable impact
Vendor risk	Static documentation	Live dependency view
Performance issues	Reactive troubleshooting	Context-aware diagnosis

Services

System & Infrastructure Inventory Service

A current, real-time view of systems and services.

A trusted system of record.

Incident & Impact Analysis

Understand what failed and what is affected.

Faster recovery.

Compliance & Audit Support

Maintain defensible, auditable records.

Reduced regulatory risk.

Third-Party Risk Visibility

Understand dependencies across vendors.

Reduced systemic

Change Impact Review

Understand what will break before deployment.

Safer releases.

Performance & Availability Review

Identify root cause and system bottlenecks.

Improved uptime.

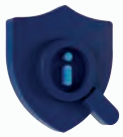
Where this service applies in financial environments

In financial environments, risk does not stay in one place. A service issue can spread across connected systems. A breach can begin with an asset no one realized was still exposed. A vendor problem can affect more than one workflow. A routine change can disrupt services far beyond the original target.

A system outage spreads across multiple services.

Dependencies are not visible.

Read: Why two-thirds of outages start outside your systems



A breach starts from an unknown system.

Inventory is incomplete.

Read: Why environment visibility is the riskiest assumption we make

A third-party failure impacts multiple systems.

Connections are not mapped.

Read: Why two-thirds of outages start outside your systems

A change causes unintended disruption.

Impact was not understood.

Read: Why environment visibility is the riskiest assumption we make

These are the moments where partners can step in with repeatable services—not just one-time fixes.

When to bring this to a financial client

This service is easiest to introduce when the client is already feeling the impact of limited visibility.

That often happens when:

- Audits or regulatory reviews begin
- Outages or disruptions occur
- Security risks are identified
- Infrastructure changes are planned
- Third-party risk is under review

You can also start with questions like:

- Do you have a complete, current view of your systems?
- Can you map dependencies across systems and vendors?
- Can you trace impact during an incident?
- Do teams work from the same data?
- Can you prove your environment is under control?

How to package this as a recurring service

Month 1 — Establish the baseline

- Build system inventory
- Map dependencies
- Identify risks

Monthly — Keep it current

- Track changes
- Monitor risk
- Maintain visibility

Quarterly — Support decisions

- Support audits
- Plan changes
- Optimize systems

What this helps partners deliver

- Faster incident response
- Improved uptime
- Reduced regulatory risk
- Better decision-making
- Clearer visibility into risk
- Stronger client trust

Why this makes you harder to replace

- You maintain the most trusted view of the environment
- You reduce uncertainty during incidents
- You guide decisions over time

Delivered through your experience, this value stays with you.

How to start with an existing financial client

Start with one client dealing with:

- Audit pressure
- Security concerns
- System complexity
- Visibility gaps

Then:

- Focus on one use case
- Build visibility
- Solve one problem
- Expand into recurring services

Start building your financial services practice

Apply to the Technology Advisor Partner Program

www.wanaware.com

Version 1.1 — 2026