

The FSI resilience blueprint: Maintaining control when upstream systems fail

Outages are inevitable. Systemic collapse is not. Here is how leading institutions minimize downtime, empower incident response, and satisfy regulators during unexpected disruptions.



High cost of interruption

\$152M

estimated annual downtime cost for financial services firms

[Splunk](#)

71%

of FSI leaders report critical app outages cost \$1M or more per hour

[New Relic](#)

\$2.2M

median hourly outage cost in financial services

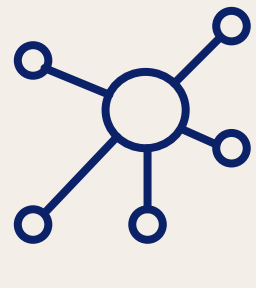
[New Relic](#)



More than 70% of organizations have launched operational resilience initiatives

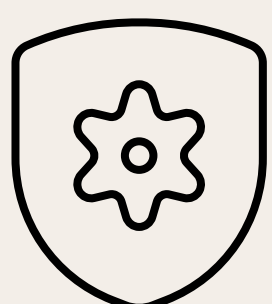
[Business Continuity Institute \(BCI\)](#)

Six elements of a modern resilience model in FSI



1 Map ecosystem fragility

Why it matters: Interdependencies across identity, SaaS, APIs, and third-party vendors mean a single failure can cascade instantly. Proactively mapping these vulnerabilities shortens the blast radius and prevents localized glitches from becoming systemic failures.



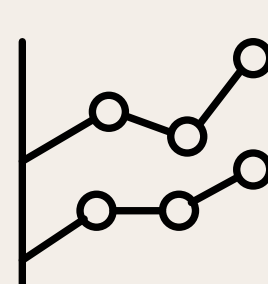
2 Safeguard IT responder access

Why it matters: When primary infrastructure goes dark, your incident response teams cannot be locked out of the environment. An independent, secure access layer (like the one provided by the Citrix platform) ensures your IT “heroes” can immediately reach critical systems to diagnose and repair issues — drastically cutting Mean Time to Resolution (MTTR).



3 Enforce crisis governance

Why it matters: Emergency “break-glass” access shouldn’t trigger privilege drift or audit exposure. Dynamic, policy-driven controls ensure IT responders have exactly the access they need to fix the issue, without spiking your compliance risk during a crisis.



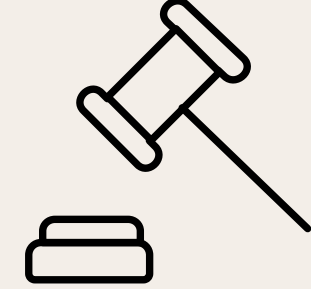
4 Deploy contextual telemetry

Why it matters: You can’t fix what you can’t see. Prioritized, contextual telemetry speeds up detection and isolates issues instantly, giving your remediation teams real-time visibility while capturing the exact forensics regulators demand.



5 Execute rapid rollbacks

Why it matters: Human error and misconfigurations frequently occur during high-stress incidents. Validated, instant rollback capabilities restore stable, “known-good” operation in a few clicks, protecting FSI market continuity.



6 Deliver audit-ready evidence

Why it matters: Surviving the outage is only half the battle; you must survive the post-mortem. Tamper-proof logs and concise reporting [prove to auditors and regulators](#) that you maintained complete governance and control throughout the disruption.

The bottom line

Modern FSI resilience isn’t about hoping an outage never happens — it’s about ensuring you maintain secure control and compliance when it does. The Citrix platform provides the digital access layer that makes this framework possible.



How to get started with Citrix

Need help mapping your environment? Schedule a 30–45-minute whiteboard session with your Citrix account team to identify the gaps most likely to extend downtime — and the actions that can help reduce recovery time fastest.