

Keeping the business running through disruption

From partial failure to controlled impact — a five-stage operating model for CIOs



The cost of disruption

24% of customers leave after one bad experience – 70% leave after two.
Resiliency is no longer an IT concern – it’s a leadership discipline measured in revenue protection, trust and regulatory confidence.

55%

of companies face outages at least once per week

[Cockroach Labs](#)

\$1.9M

hourly cost during high-impact outages (77 hrs median/year)

[New Relic](#)

4.88M

average cost of a data breach in 2024

[IBM Security](#)

The resiliency journey

Five stages from strategic intent to proven, repeatable resilience

Stage one

Stable entry point for Tier 0–1 work

Business need
Critical work must stay reachable through a consistent front door when core services are under stress

Citrix impact

- Users have one place to access priority apps, desktops, SaaS, and private web workflows
- Hybrid and multi-cloud delivery so work can shift across environments when a hosting path degrades

Business outcome: Less confusion, fewer risky workarounds, and less helpdesk surge during disruption

Deutsche Bahn standardized access to critical work, delivering a 30% efficiency improvement, ~40% operating cost reduction, and one-day onboarding/offboarding.

Stage two

Flexibility across cloud and identity dependencies

Business need
Organizations need continuity when cloud regions, identity paths, or upstream dependencies partially fail

Citrix impact

- A multi-cloud and multi-identity platform so critical work is not trapped in a single delivery path
- Intelligent traffic management, controlled failover, and service continuity for critical applications

Business outcome: Lower concentration risk and better continuity through partial failures (rather than waiting for full recovery)

Severn Trent improved stability for tier-zero critical services and cut provisioning times from months to minutes.

Stage three

Controlled access for employees and partners

Business need
Continuity should not require broad network access or unmanaged exceptions for employees, contractors, partners, and third parties

Citrix impact

- Apply zero-trust, least-privilege access to private applications without broad VPN-style exposure
- Control third-party access paths so the business can continue operating while limiting blast radius

Business outcome: Safer continuity during incidents, audits, and vendor-related disruptions

Mass General Brigham uses Citrix to securely deliver virtual apps at scale, supporting flexible, resilient healthcare access.

Stage four

Safe fallback for web/SaaS apps and unmanaged devices

Business need
When browser-based workflows become the fallback, organizations still need policy, containment, and evidence

Citrix impact

- Creates a policy-controlled lane for web and SaaS work
- Contain data movement and reduce leakage risk on unmanaged or BYO devices

Business outcome: Work continues with tighter controls instead of loosening policy in the name of speed

How **Citrix** has standardized secure access to support scalable, efficient operations for a European energy provider.

Stage five

Faster detection, auditability, and rollback

Business need
Leaders need to detect impact quickly, prove control during disruption, and restore services to known-good states faster

Citrix impact

- Improve visibility into sessions, app delivery, and user experience so teams can triage faster
- Preserve evidence and turn recovery into a repeatable operating motion instead of manual improvisation

Business outcome: Shorter time to detect, stronger auditability, and faster restoration to known-good states.

A **Big 5** accounting firm used a two-region design that eliminated hours-long restore windows and brought teams online in hours, not weeks.

The bottom line

Resilience is now audited and judged publicly. Leaders win by keeping critical services running safely during disruption, with proof that stands up to regulators, boards, and customers.

Business resiliency is no longer about getting systems back online. It's about keeping the business running while they're not.

