Perspective

Resilience in motion

Why banks and insurers need a new model for changing critical services under regulatory pressure.

The next measure of resilience is the confidence to change.

Content

Executive summary

Leaders across technology, operations, security and risk in banking and insurance are being asked to change more and prove more at the same time.

Legacy environments need to be modernized. Cloud architectures continue to evolve. AI is entering processes that matter to customers, risk and operations. Cyber threats keep changing. Critical services increasingly span external providers, platforms and subcontractors.

At the same time, the standard for operational resilience is rising. DORA has made ICT risk management, incident management, resilience testing and third-party risk part of a common European framework. Banks and insurers need to demonstrate that critical services are understood, controlled, tested and recoverable, including the dependencies that sit outside their own organization.

For a CIO, COO, CISO or CRO, these pressures converge around the same object: the critical service. Every significant change creates a corresponding need to establish confidence that the service remains under control.

> The most resilient financial institution is not simply the one that can withstand disruption. Increasingly, it is the one that can change critical services with confidence.

That changes the role of resilience. Assurance needs to keep pace with change, operational evidence needs to be easier to use, and scarce expertise needs to focus on material decisions rather than repeatedly reconstructing proof. The result is a different relationship between transformation and resilience: resilience becomes part of how change moves forward.

Regulation is changing the transformation equation

Modernization in banking and insurance carries a significant control burden. What is changing is the extent to which technology transformation and operational resilience now have to be managed together.

Critical services increasingly depend on combinations of applications, infrastructure, cloud, data and external providers. The underlying business process may span multiple systems and legal entities. Yet the institution remains accountable for understanding how that service works, where its material dependencies sit and how it recovers when something goes wrong.

DORA makes this connection more explicit. Operational resilience now reaches into ICT risk, testing, incidents, out-sourcing, ICT third-party risk and oversight of critical ICT third-party service providers. Every modernization initiative therefore has two parallel require-ments: the technology has to work in its target state, and the institution has to establish that the target state remains governable, recoverable and sufficiently transparent.

That second requirement can become a hidden source of friction. A platform may be technically ready while confidence in the changed service still depends on control ownership, evidence, recovery testing, supplier transpa-rency and escalation paths.

> The problem is not simply the pace of technology change. It is the ability of assurance to keep pace with it.

A useful lens

Assurance latency

The delay between changing a critical service and regaining confidence that it remains controlled, recoverable and transparent.

Signs of assurance latency

- Critical changes are technically complete before assurance is ready.
- Evidence is repeatedly reconstructed for audits, risk reviews or due diligence.
- Recovery assumptions no longer reflect the service as it operates today.
- Provider and subcontractor dependencies become visible too late.

The greater the latency, the more assurance can become friction on the next change.

The new resilience equation.

Resilience in motion

The ability to keep changing without losing confidence in control.

The challenge
When assurance doesn't scale with change, confidence becomes the constraint.

The opportunity
Build critical services that are always ready for what's next.

Banking insight

Change windows are getting tighter while assurance requirements are getting broader.

Payments, trading, treasury and capital-markets platforms combine high availability requirements with complex interfaces, restricted change windows, incident transparency and demanding evidence expectations.

Insurance insight

Resilience increasingly follows the customer journey, not the system boundary.

Policy administration, claims, underwriting and investment services often depend on integrated applications, data flows and external providers. The relevant question is whether the business service can continue and recover across those dependencies.

Resilience becomes the confidence to change

Traditional resilience disciplines remain essential. Institutions need reliable systems, effective business continuity, tested recovery procedures and strong incident management. But stability alone is no longer a sufficient measure of resilience.

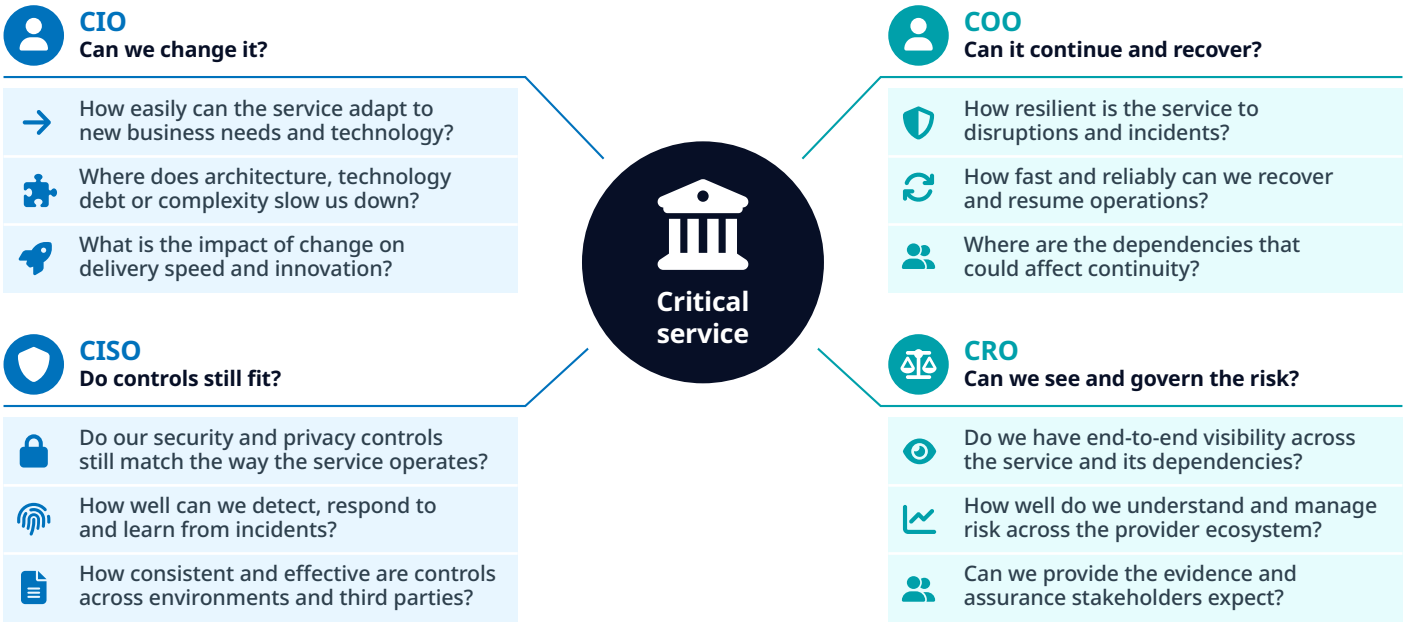
A bank or insurer may be able to keep today's environment running reliably and still struggle if every material change triggers a lengthy cycle of additional assessment, control design, evidence gathering and coordination before the organization is comfortable enough to move forward.

> How quickly can we change a critical service and regain confidence that it remains under control?

That question turns resilience into a transformation capability. A resilient change model brings operational, security and regulatory considerations into the service early enough that they do not have to be reconstructed later. Controls connect to the actual delivery model. Recovery assumptions are tested against the current service. Evidence is generated closer to the activity it is meant to prove.

One critical service. Four executive perspectives.

Resilience is a shared leadership agenda



One critical service, four executive perspectives

CIO Can we change this service without rebuilding confidence from scratch?

COO Can the service continue and recover across the full business process?

CISO Do security and recovery controls still match the service as it changes?

CRO Can we see and govern the material risk across providers and dependencies?

The roles see different dimensions of the same service. A stronger resilience model gives them a shared basis for deciding how much change the institution can absorb while remaining in control.

From audit ready to always ready

One of the clearest signs that assurance has not yet caught up with the operating model appears when an audit, regulatory review or due-diligence request arrives.

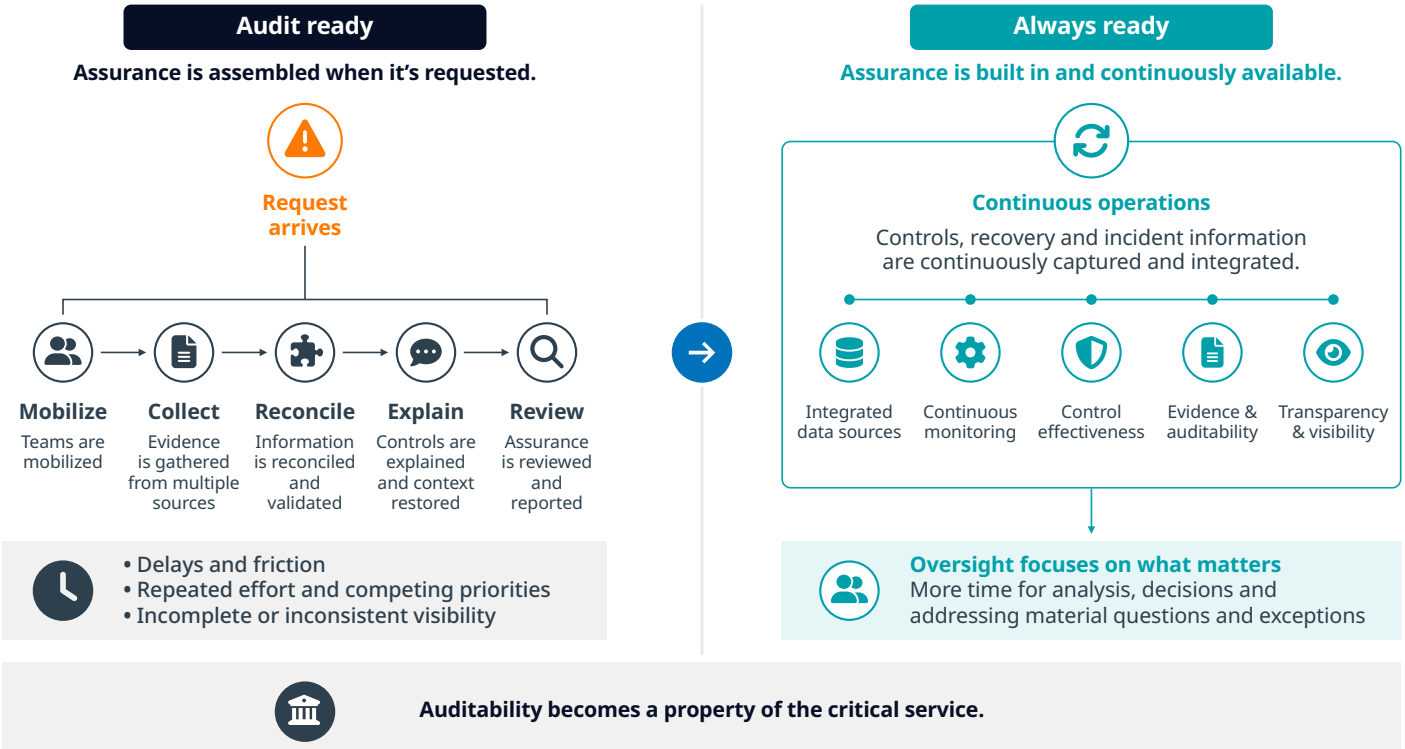
Teams mobilize. Evidence is requested from different parts of the organization and from providers. Controls are explained again. Records are assembled. Similar information may be requested repeatedly in slightly different forms. The underlying controls may be working well; the friction lies in turning their operation into usable assurance.

The deeper opportunity is to move from audit ready to always ready. Always ready does not mean continuous auditing or more dashboards. It means designing critical services so that the information required for effective oversight is easier to obtain, interpret and trust.

That may include current control status, evidence freshness, recovery-test results, incident information, remediation progress and material changes in the provider ecosystem. Formal audits remain important, but they become one consumer of a more continuous assurance flow rather than the moment when that flow has to be rebuilt.

From audit ready to always ready.

A shift from episodic evidence collection to continuous assurance



Auditability becomes a property of the critical service, rather than a recurring exercise around it.

Banking insight

Evidence should be ready before the review asks for it.

For a critical payments or trading service, access reviews, change records, recovery tests and incident information can be organized around the service and made easier to use before a formal review begins.

Insurance insight

Assurance has to follow the service across systems and partners.

For claims, policy or investment services, assurance may need to span integration, data quality, reporting and service continuity across multiple systems and providers.

The value of resilience shows up in speed, risk and capacity

A better assurance model matters because the cost of resilience is broader than the compliance budget.

Transformation speed

When every change requires substantial additional work to establish the relevant controls, evidence and governance, time-to-value extends beyond the technical implementation. Reusable assurance structures and proven delivery patterns can reduce the amount of design and verification that has to start from zero each time.

Risk and control visibility

Executives can make better decisions when control status, recovery readiness, dependencies and remediation are more visible around the critical service. The objective is not to generate more reporting. It is to reduce uncertainty about the current state of the service and where management attention is required.

Expert capacity

Operational resilience depends on people who understand technology, operations, security, risk, architecture and regulation. In many institutions, those same experts are also required to prepare evidence, coordinate providers and respond to recurring control questions.

> Your best people should be shaping what comes next, not repeatedly proving what already happened.

The resilience dividend therefore appears across three dimensions: transformation can move with less assurance friction; risk and control become more visible around the service; and specialist capacity can shift toward material decisions, exceptions and complex remediation.

Accountability stays with the institution – Assurance becomes more networked

No provider can take regulatory accountability away from a bank or insurer. The institution remains responsible for its regulatory obligations, risk decisions and supervisory relationships.

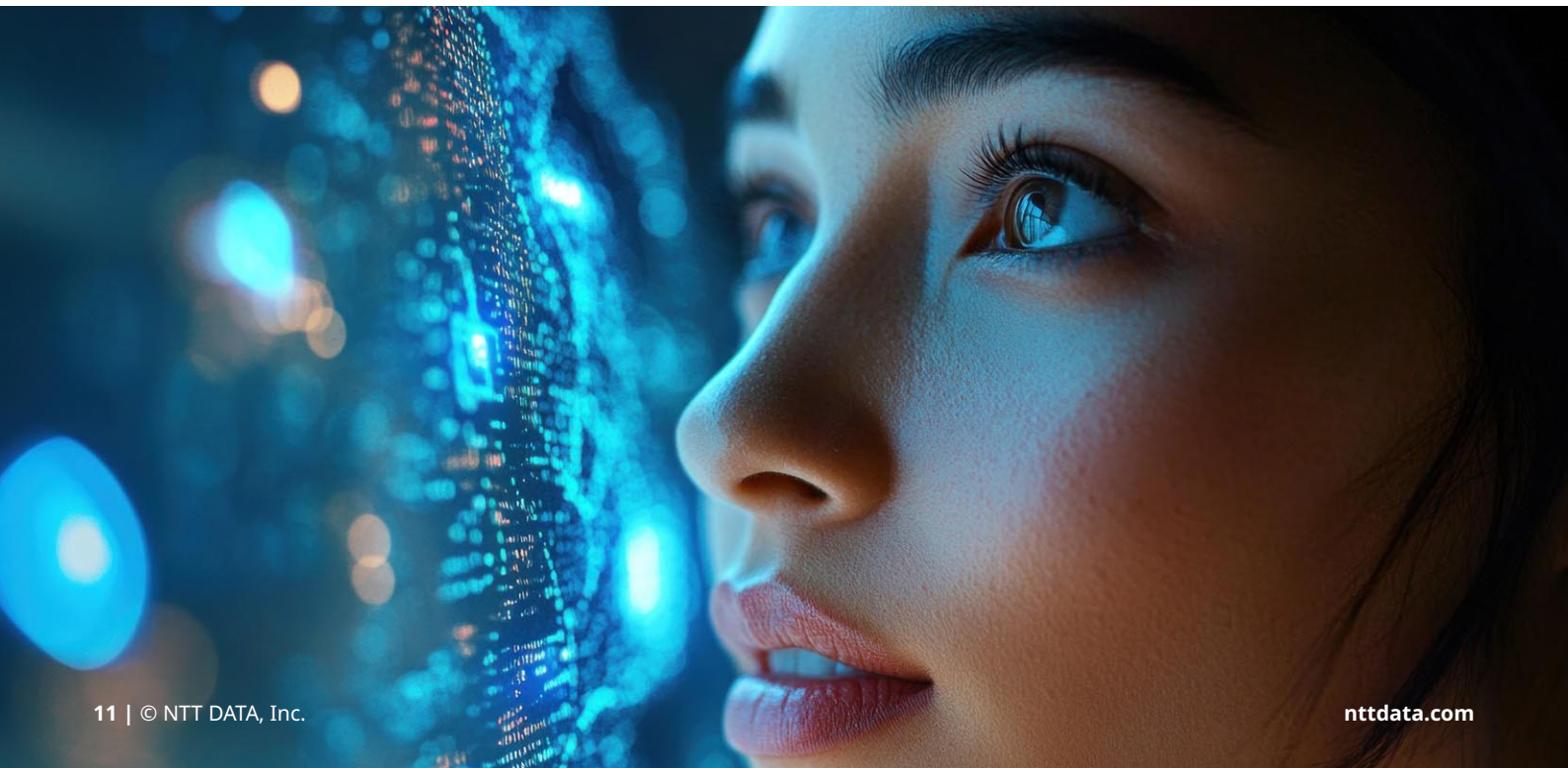
What can change is the division of work required to exercise that accountability. A provider contributing to the operation or change of a critical service is close to many of the activities that create assurance: access management, change, incident handling, recovery testing, service reporting and subcontractor management.

When relevant evidence and control information are created as part of operating the service, they can become structured inputs into institutional oversight. This is what we mean by networked assurance: organizational boundaries remain clear while the information needed for technology, operations, security, risk and audit decisions moves more effectively across them.

For a CIO, that can reduce friction around change. For a COO, it can improve visibility into continuity and recovery. For a CISO, it can make security and resilience evidence easier to connect to the current service. For a CRO, it can improve the basis for risk-based oversight across providers and dependencies.

The organizational boundaries remain. The information flows improve.

The opportunity is therefore not to add another governance layer. It is to make existing governance more scalable as critical services become more distributed and more frequently changed.



The role of a strategic resilience partner

As the resilience challenge changes, the role of the technology provider changes with it. For critical services, technical delivery alone is no longer enough. Institutions increasingly need partners that can contribute to control, recoverability, transparency and assurance as part of how services are transformed and operated.

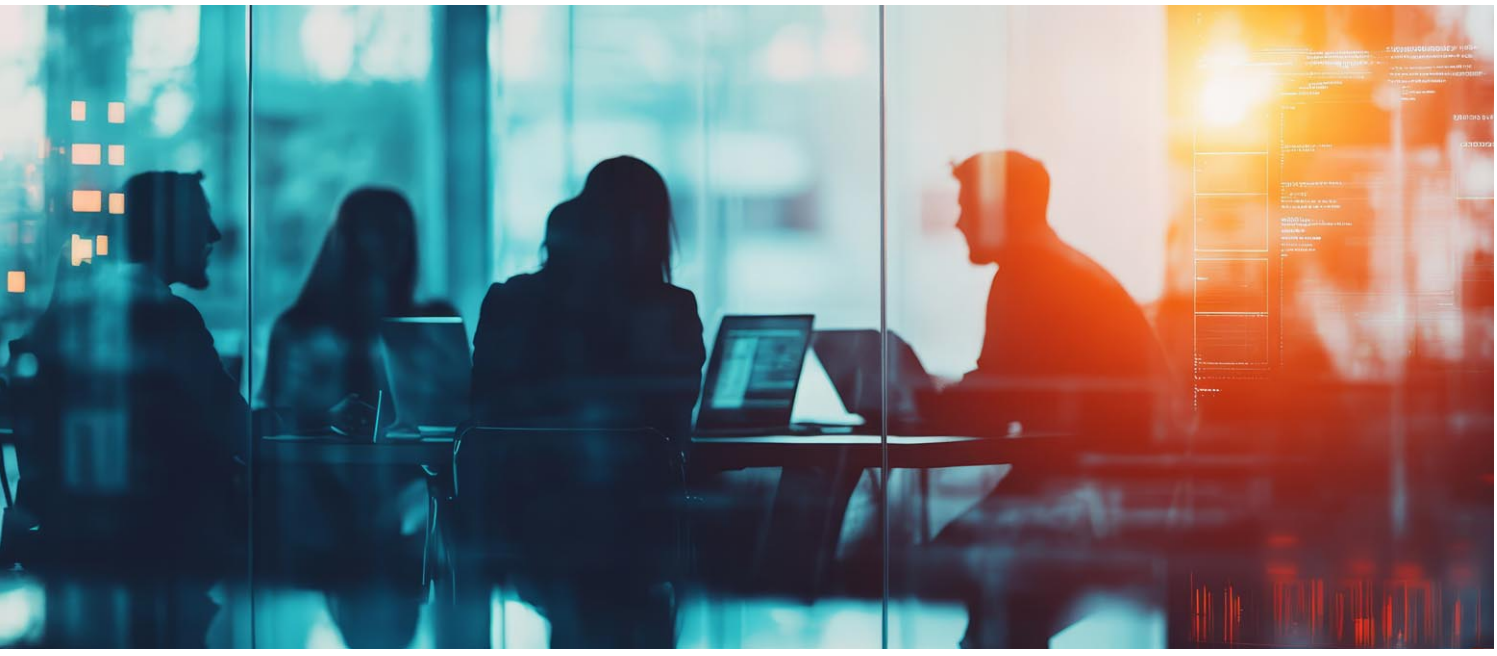
This does not imply a standard blueprint. Every bank and insurer has its own critical services, risk appetite, control framework, supervisory context and provider landscape. The value of a strategic resilience partner lies in combining repeatable experience with the institution-specific decisions that remain with the client.

NTT DATA approaches this role by bringing together banking and insurance expertise with technology transformation, managed operations, cyber resilience, cloud, data, AI and regulatory understanding. Our Resilience Assurance approach is designed to help connect these capabilities around the critical service rather than treat resilience as a separate workstream added after the technology has changed.

In practice, the conversation is less about introducing another tool or governance framework and more about agreeing what good looks like for a specific service: which resilience outcomes matter, what needs to remain visible, where accountability sits and how provider activity can contribute usable assurance.

> A strategic resilience partner helps the institution change critical services with greater confidence while keeping accountability where it belongs.

The useful starting point is the operating reality of the service, not a predefined package.



Which critical service would you choose?

Every institution has services where regulation, technology change and operational dependency meet. It may be payments, trading, claims, underwriting, policy administration, insurance investment operations, a critical data platform or another service undergoing significant change.

Take one of those services and look at it through the resilience in motion lens:

- How much effort does it take to establish confidence after a material change?
- Is assurance information produced through normal operations, or reconstructed when someone asks for it?
- Can we see the third- and fourth-party dependencies that materially affect the service?
- Do our recovery assumptions reflect the service as it operates today, rather than how it was originally designed?
- Where are scarce technology, operations, security and risk experts spending time on repeatable assurance work?

An invitation to talk

The conversation starts with one critical service.

To discuss how this perspective applies to one of your critical services, please contact:

Andreas Seibert
Head of BFSI Regulatory & Compliance DACH
NTT DATA
andreas.seibert@nttdata.com

NTT DATA works with banking and insurance leaders to explore these questions around the services that matter most to their institution. The discussion starts with your operating reality and the change you are trying to make, then looks at where greater confidence, visibility and resilience could reduce friction across technology, operations, security and risk.

Regulation may have created the trigger. The opportunity is broader: to make resilience part of the institution's ability to keep changing while remaining in control.

Which critical service would you choose?

Visit **nttdata.com** to learn more.


NTT DATA