

Insight report

Assured Science: From Discovery to Delivery

Why resilient, observable networks matter across global life sciences

What life-sciences discussions and independent industry evidence reveal about the networks supporting pharmaceutical research, manufacturing operations and global supply chains.

Explore the report

Evidence and methodology

This report examines network resilience across the global pharmaceutical and life-sciences value chain, from research laboratories and development teams to manufacturing sites, quality functions and distribution partners. Its scope is enterprise and inter-site connectivity, critical application access, the visibility of network services and the coordination of providers. It does not assume a managed network partner operates laboratory instruments, production control systems or regulated quality processes.

Our audience research used AI-assisted profiling and inferential analysis to classify 44,733 publicly expressed online opinions associated with senior enterprise technology, infrastructure and network leaders in pharmaceutical and life-sciences organizations. The discussions were drawn from X, Quora, Reddit, Bluesky, TikTok and Threads during the 12 months ending 12 October 2026. The source methodology reports a 95% confidence interval and 5% margin of error; the applicability of those measures to inferential online-opinion modeling has not been independently validated for this report. The classifications are directional interpretations of online discussion, not direct survey responses, independently authenticated job titles or audited evidence of what organizations have deployed.

The underlying opinion sample is US-focused. The strategic discussion is designed for a global audience and draws on international and jurisdiction-specific technical guidance, which is identified as such. Different evidence sources have different populations, definitions and purposes. They should not be treated as statistically interchangeable. Selected percentages are included where they sharpen a relevant business question; they do not establish global adoption or maturity benchmarks.





Executive summary

Modern life sciences depend on a network of connected activities rather than a single site or digital platform. Research laboratories generate and exchange complex data; development and quality teams rely on timely access to records; production facilities operate sensitive systems; and global partners coordinate raw materials, specialist services and distribution. Across these activities, a network disruption can affect far more than an IT service ticket. Its significance depends on which scientific or operational process is interrupted, what data or systems become unavailable and how quickly an acceptable operating state can be restored.

Our analysis identifies a potential mismatch between the scale of these dependencies and the completeness of resilience planning. **49% of modeled opinions** suggested that R&D laboratories were somewhat less covered by network resilience plans, while another set of findings gave strong weight to independent observability platforms and the exploration of AI-assisted operations. The findings do not independently verify organizational resilience, but they point to a useful leadership question: are the most important activities across the pharmaceutical value chain supported by demonstrably resilient, observable and accountable connectivity?

The answer is unlikely to be a single networking product or a uniform architecture. Different sites operate different systems and risk profiles. A research campus may depend on collaboration and cloud analysis, a manufacturing plant on tightly controlled production data paths, and a distribution operation on transaction and tracking services. Resilience therefore needs to be defined around critical outcomes, supported by consistent information and managed across the suppliers and organizational boundaries on which those outcomes rely.

Five connected priorities emerge from the research, highlighting the capabilities needed to support scientific and operational continuity across global life sciences:

1. **Follow critical workflows across the lifecycle.** Identify the applications, data transfers, sites and partners essential to research, quality, manufacturing and supply.
2. **Close resilience coverage gaps.** Make laboratories and distributed teams part of tested continuity arrangements, rather than assuming that central IT coverage is sufficient.
3. **Coordinate global connectivity and ownership.** Apply consistent service requirements and escalation processes without forcing every site into the same network design.
4. **Turn visibility into operational assurance.** Use meaningful performance and incident evidence to understand whether critical activities can continue and recover.
5. **Introduce intelligent operations responsibly.** Build AI and edge capabilities on trusted information, validated dependencies, engineering judgment and controlled change.

The central argument is that life-sciences network resilience should be judged by the continuity and integrity of the services it supports, not simply the availability of circuits, the deployment of a technology or the number of dashboards an organization operates.



Why this matters

For pharmaceutical and life-sciences leaders, disruption can affect experiments, analytical workflows, manufacturing coordination, batch documentation and the movement of products through external partners. These activities vary in criticality and applicable regulatory requirements, but all benefit from understanding the links between their digital dependencies and their operational consequences.

The strategic opportunity is to connect laboratory and production requirements with a coherent enterprise network operating model. That means establishing which services must be protected, what constitutes acceptable performance, who is accountable across internal and external teams, and how continuity can be demonstrated rather than assumed.

The mission is to build confidence that critical scientific and operational work can continue, recover and improve as organizations expand their digital capabilities and global partnerships, while protecting data integrity, product quality and the patient outcomes that ultimately depend on them.

Expereo perspective:

The unit of resilience is changing

Most pharma network plans still start with a site list. That's the wrong unit. A batch release, a stability study or a dataset moving to a CRO is what needs protecting, and each of those runs across several sites, clouds and providers. Over the next few years I expect leaders to stop asking whether the circuit is up and start asking whether the workflow can carry on, and whether they can prove it.

Jean-Philippe Avelange
Chief Information Officer,
Expereo



Theme 1:
Resilience must follow the pharmaceutical value chain

The starting point is the work that connectivity enables, not the number of sites connected.

The pharmaceutical value chain connects activities with very different technical and operational profiles. Research laboratories move instrument outputs and datasets between local systems, collaboration platforms and specialist analysis environments. Development and quality functions rely on validated applications and trustworthy records. Manufacturing sites may combine enterprise IT services with operational technology that must remain safe and controlled. Supply and distribution functions depend on accurate information across carriers, warehouses, manufacturers and external partners.

These functions do not share one universal tolerance for disruption. An interruption to a non-urgent research transfer may be manageable through queuing and later synchronization. A loss of access to information required for an active production or release process may need immediate intervention and controlled alternative procedures. Network strategy becomes more useful when it distinguishes these circumstances rather than imposing the same generic availability target on every application.

Define continuity around critical scientific and operational services

The ICH Q9(R1) Quality Risk Management guideline offers an important foundation for this distinction. It sets out a risk-based approach across pharmaceutical development, manufacturing and distribution, with the level of effort and formality proportionate to the potential impact on product quality and patient protection. It is not a network engineering standard. Its relevance here is the principle that infrastructure choices should be informed by the risks to the activities and outcomes being supported.

Applied to network planning, that means starting with critical workflows. Which laboratory systems depend on a central data repository? Which manufacturing records require continuous or time-bounded access? Which quality processes rely on cloud applications or outsourced testing? Where does a supply-chain information exchange depend on one identity service, one connectivity path or a provider outside the organization's control? Mapping these dependencies makes resilience investments more precise.

Connected activities: illustrative service-dependency view

Discovery Research & data → **Development** Quality & trials → **Manufacturing** Production & records → **Delivery** Distribution & partners

Network performance | service ownership | data integrity | recovery evidence

Illustrative service-dependency model

Editorial diagram developed for this report. It is not a regulatory framework or a claim that a network provider owns every process.

A practical dependency map should distinguish local infrastructure, wide-area connectivity, cloud services, applications, people and external partners. It should also identify what can continue locally when an external link fails. These are design decisions that must be agreed with laboratory, production and quality owners, not inferred from a network topology diagram alone.

Protect data integrity and controlled operations, not only uptime

The ICH Q10 Pharmaceutical Quality System guideline places emphasis on knowledge management, change management, monitoring and the responsibilities associated with outsourced activities. Its principles help explain why connectivity changes can require coordination beyond IT: a restored connection is not necessarily proof that an affected workflow or record exchange has resumed correctly.

For computerized systems used in regulated contexts, appropriate validation and data-governance requirements are essential. The ISPE GAMP 5 guide, second edition provides a risk-based good-practice approach for systems that must be fit for intended use. Similarly, the current EU GMP Annex 11 on Computerized Systems addresses risk management, data, security, backup and restoration for systems within its EU GMP scope. Neither publication means that every network service is itself a validated GxP application; rather, they underline the need to understand where network dependencies affect regulated processes.

Availability, integrity and recoverability should therefore be assessed together. A laboratory application may be reachable while results cannot be synchronized correctly. A manufacturing site may regain its Internet service but still require verification before an interrupted process restarts. The right operational response includes both technical restoration and confirmation by the responsible process owner.

Extend the view to external partners and supply chains

The OECD's 2026 research on medical supply chains documents the visibility challenges and dependencies that complicate the supply of medical products, including upstream inputs and cross-border operations. Its analysis focuses on European supply chains, but the broader lesson is that information flows and operational dependencies extend beyond a single organization's facilities. Connectivity planning should recognize those boundaries without claiming network resilience alone can prevent medicine shortages. A 2026 World Economic Forum analysis of pharmaceutical cyber resilience similarly highlights that disruption can extend beyond IT restoration to affect production, batch release and medicine availability. This is industry commentary, not an independent measurement of network-failure frequency.

A pharmaceutical company may coordinate with contract research organizations, contract manufacturers, testing laboratories, distribution providers and cloud platforms, each operating different technology and support arrangements. A failure at one link can create delays whose causes are not obvious from the parent organization's own network view. Ownership, alternative procedures and escalation contacts therefore matter as much as connection specifications.

Strategic insight

Life-sciences network resilience begins with a clear view of the scientific and operational activities that must continue, the digital dependencies supporting them and the consequences when those dependencies fail.

For leaders, this means moving beyond site-by-site connectivity plans toward an evidence-led understanding of critical services across the pharmaceutical lifecycle. Infrastructure decisions should be assessed through their contribution to research continuity, controlled operations, data integrity and effective recovery, with the relevant quality and business owners involved in defining success.

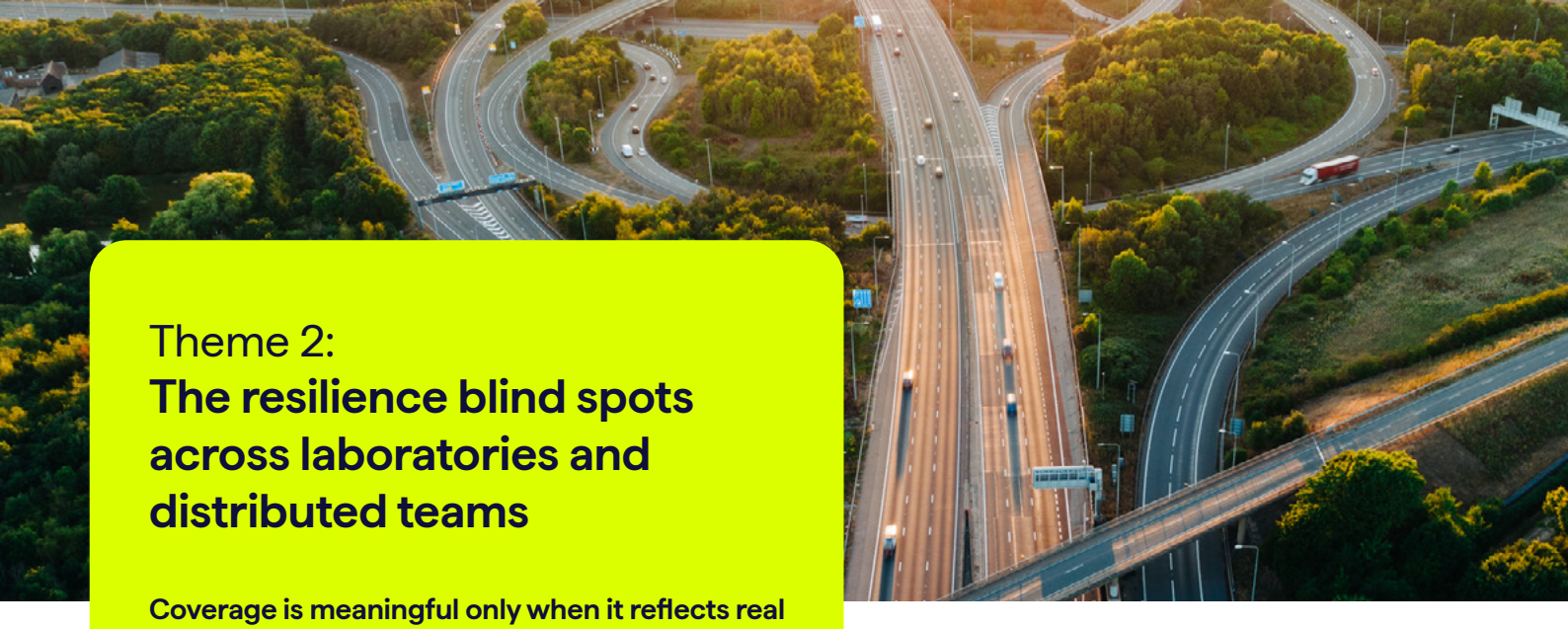
Once these dependencies are established, the next question is whether resilience plans cover every critical part of the estate, particularly laboratories and distributed teams that may sit outside standard enterprise-network arrangements.

Expereo perspective:

Map dependencies with the people who do the work

A laboratory can complete a test while a manufacturing site is still waiting for the result needed for batch release. The dependency can span several organizations, applications and identity services. Resilience planning needs to follow that process across company boundaries. The critical connection may carry very little data, but its failure can delay a decision that holds up an entire batch.

Julian Skeels
Chief Digital Officer, Expereo



Theme 2:
The resilience blind spots across laboratories and distributed teams

Coverage is meaningful only when it reflects real dependencies and has been tested in practice.

Research laboratories and distributed workers can fall between conventional categories of network and business-continuity planning. Laboratories may have specialized instruments, local data stores, long-running experiments and collaboration requirements that differ from office IT. Remote researchers, quality specialists and external partners may need access through varied locations and devices. These environments can be central to organizational outcomes even when they are not managed through a standard corporate-site blueprint.

What the research suggests about laboratory coverage

Our analysis classified **49% of modeled discussions** as suggesting that R&D laboratories are somewhat less covered by network resilience plans, while **28%** were associated with laboratories being mostly covered. These are separate opinion classifications within a wider research question, not an audited inventory of laboratory continuity arrangements. They should not be read as evidence that a specific proportion of laboratories lack protection.

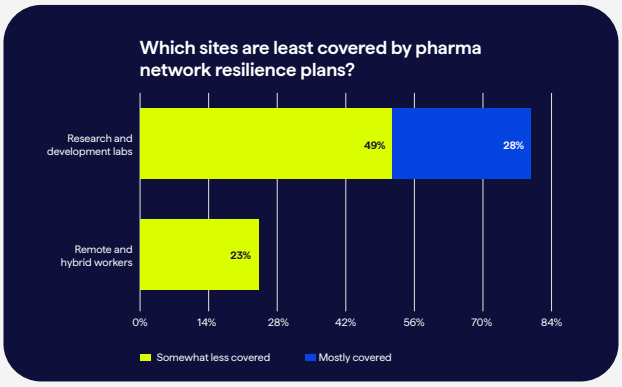


Figure 1. Perceived laboratory resilience coverage

Nevertheless, the distinction is useful. Laboratories can depend on both local services and external resources: identity systems, data repositories, cloud analysis, specialist software licenses, instrument-support connections and collaboration platforms. A central continuity plan may describe network restoration at the campus level without establishing how a disrupted experiment, analytical workflow or research dataset will be recovered.

Effective resilience planning should therefore identify which laboratory activities are time-sensitive, which can operate safely offline and which require verified data reconciliation after service returns. The answer is often a mix of network paths, local procedures, application safeguards and human decision-making. Resilience cannot be measured solely by the presence of a secondary circuit.

Include remote teams and connected research partners

A separate finding classified 23% of opinions as indicating that remote and hybrid workers were somewhat less covered by resilience plans. This result concerns perceived coverage, not measured security controls or workforce readiness. It matters because distributed research and quality activities often rely on identity, cloud applications, file transfer and secure access to services hosted in multiple locations.

A well-connected laboratory can still face disruption if its collaborators cannot authenticate, receive large datasets or access critical applications. Conversely, good remote access does not automatically protect the underlying research system or the integrity of exchanged data. Organizations should review both the resilience of network access and the resilience of the workflow at each end of the connection.

The UK MHRA's guidance on GxP data integrity addresses expectations for data governance across regulated pharmaceutical activities, with appropriate distinctions between GLP, GCP, GMP and other contexts. This is UK guidance, not a global law, but it is a useful reminder that availability alone does not establish whether data are complete, attributable or fit for their intended use. Similar principles are expressed in the PIC/S good practices for data management and integrity for regulated GMP/GDP environments.

Turn perceived coverage into testable assurance

The starting point is an inventory of critical services and their dependencies, validated by people who understand the work. For a laboratory, that might include scientific instruments and their interfaces, local compute, off-site storage, network routes, identity systems and support suppliers. The inventory should indicate which components are essential to continuing work, which are required to recover safely and which can tolerate a delayed return to service.

Testing should reflect plausible failure scenarios, not only confirm that a backup connection switches over. Teams might simulate loss of a research application, a campus Internet outage or an unavailable third-party data platform. They should establish whether local operations continue, whether information can be recovered accurately and who decides when the process is ready to restart. Findings should feed a prioritized improvement plan, with responsibilities documented across research, IT, security and quality functions.

For geographically dispersed organizations, one standard for documenting criticality and recovery can coexist with different local technical solutions. A laboratory handling large research data transfers may require a different design from a remote clinical-operations office, while both need clear incident ownership and evidence of recovery readiness.

Strategic insight

The resilience gap is not simply where connectivity is absent; it is where critical scientific activities and distributed users have not been mapped, assured and tested against meaningful recovery outcomes.

Pharmaceutical leaders should treat laboratories, remote teams and external research partners as part of the enterprise's critical-service landscape. Consistent assessment and testing can expose where local infrastructure, shared platforms or supplier responsibilities create fragile dependencies, allowing improvement efforts to follow operational risk rather than administrative boundaries.

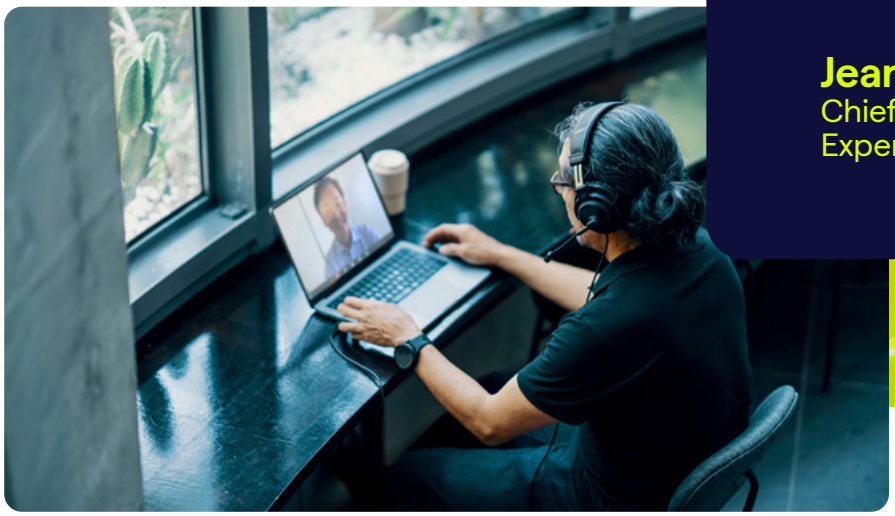
Addressing these blind spots creates the foundation for the next challenge: coordinating resilient connectivity across a wider global estate of facilities, partners and technologies.

Expereo perspective:

Test a lab like a production line

Labs are where the gap between the continuity plan and the day itself is widest. A campus can have two diverse circuits and still lose a long-running experiment because an instrument-support link or a license server sat outside the test. Rehearse a lab the way you'd rehearse a production line. Pull the plug, watch what the scientists actually do, and write down who decides it's safe to carry on.

Jean-Philippe Avelange
Chief Information Officer, Expereo





Theme 3:

Coordinating resilient connectivity across global operations

Global consistency should come from service management and accountability, not identical configurations at every site.

Pharmaceutical organizations often operate across regions, local access markets and technical generations. A research campus, an office, a production plant and a distribution center can have different requirements for bandwidth, performance, local autonomy and security. Global infrastructure teams nevertheless need to maintain coherent information about the services on which these environments depend.

The challenge is not necessarily to eliminate network diversity. A site may have only a limited choice of access providers, while another may use several carriers for resilience. A manufacturing facility may maintain a locally controlled environment for sensitive operational technology, while enterprise applications and shared data services depend on managed wide-area and Internet connectivity. These layers are related, but they should not be treated as interchangeable solutions.

Standardize how services are specified, owned and restored

A coordinated network operating model should define common service information: site and application criticality, approved connectivity options, provider contacts, performance baselines, change procedures, incident escalation, restoration priorities and evidence required after service changes. This makes a global estate easier to operate without prescribing the same access technology everywhere.

For example, a central networking team may manage regional connectivity providers, a managed SD-WAN service, cloud access and security partners while local IT or engineering personnel retain responsibility for site-specific equipment. The operating model should identify who can detect a fault, who can change routing, who authorizes changes affecting critical processes and who confirms that the business service has recovered.

The ICH Q10 guideline recognizes that outsourced activities require defined processes and responsibilities within the pharmaceutical quality system. That principle does not make a connectivity provider responsible for pharmaceutical quality decisions, but it reinforces the need for manufacturers to document where supplier services support regulated operations and how relevant changes or incidents are managed.

Use SD-WAN as a capability, not a maturity claim

Software-defined wide-area networking can help apply common traffic policy, select among suitable network paths and improve central visibility across geographically distributed sites. In the right operating model it may reduce administrative complexity or help maintain application access during certain path failures. These are potential capabilities, not proof of resilience by deployment alone.

The decision should begin with a map of application needs, available physical paths, service criticality and recovery dependencies. Some locations may need local autonomy, alternative access technologies or stronger physical route diversity. An SD-WAN overlay cannot resolve a shared upstream failure, an unavailable application or an incorrect recovery procedure by itself. Deployment is therefore a design choice to test against operational requirements, not a measure of resilience maturity.

For buyers, the relevant evidence is operational: measured performance on critical paths, tested restoration scenarios, consistency of service ownership, support response across regions and the ability to adapt as a site or partner arrangement changes. This is more useful than comparing feature checklists without understanding the underlying services.

Build the network plan around the wider partner chain

Contract manufacturing organizations, specialist laboratories, logistics firms and cloud providers may each manage their own infrastructure. The OECD's 2026 medical supply-chain analysis highlights the fragmented information and cross-border dependencies in medical supply chains. At a network level, the practical response is to identify the digital exchanges and external services whose failure would affect priority activities, then determine the available monitoring, escalation and alternative arrangements.

The absence of one supplier contract does not necessarily create risk; diverse providers can be useful. Risk becomes harder to manage when a global organization cannot see service relationships, distinguish fault domains, obtain comparable incident information or coordinate changes across several partners. A managed operating model can add value by improving accountability and the speed of diagnosis, without pretending to control every third-party component.

New-site and partner onboarding should also be repeatable. Early checks of local carrier availability, required security boundaries, application needs, testing windows and support ownership can reduce preventable handovers. Acceptance criteria should be tied to the services expected to work after launch, not simply the date on which a circuit was delivered.

Strategic insight

Scaling resilient life-sciences connectivity depends on a coordinated operating model that brings visibility, performance expectations and clear ownership to diverse facilities and providers.

For global leaders, the priority is to standardize the information and governance needed to deliver dependable services while retaining local flexibility for research, manufacturing and distribution. Resilience is strengthened when teams know which services matter, which partner owns each dependency and what tested recovery looks like across the full-service chain.

That shared operating model creates the conditions for moving beyond reactive fault handling toward more meaningful network observability and evidence of service performance.

Expereo perspective:

Local choice, global accountability

A global pharma estate will never be uniform, and it shouldn't be. One plant has a single local carrier, a research hub elsewhere has four to choose from. What should be uniform is how every service is specified, owned and restored. When one partner holds the contacts, baselines and escalation path across up to 190 countries, a site team under pressure makes one call. Over time that consistency matters more than any single technology choice, SD-WAN included.

Matthew Lea
Product Development Director, Expereo





Theme 4:
From network visibility to operational assurance

Observability creates business value when technical information helps explain disruption and recovery in critical services.

Network health dashboards can indicate that circuits or devices are available, yet a research application may still be unreachable or a data transfer may remain incomplete. Pharmaceutical organizations need visibility that connects technical conditions to the services used by scientists, quality teams, manufacturing operations and external partners. Without that context, a central team may see a green infrastructure indicator while the people carrying out critical work still experience a failure.

The research places weight on independent observability

In our audience analysis, **77% of modeled opinions** were associated with finding a third-party observability platform helpful for pharmaceutical network resilience. A separate category classified **23%** as regarding an AIOps platform as essential. These are different judgments, using different strength-of-preference labels; the two categories should not be treated as competing products or as shares of a single exclusive choice.

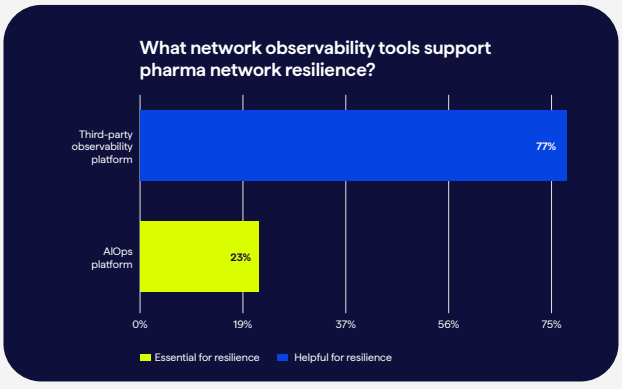


Figure 2. Third-party observability and AIOps

The finding suggests the appeal of additional visibility across increasingly complex networks. A specialist platform may help consolidate telemetry, identify degraded routes, analyzes patterns or expose the contribution of external providers. But the presence of a platform does not prove that an organization understands every service dependency or can restore an affected process. Information becomes assurance only when it supports accountable action.

For example, a laboratory may experience poor access to a scientific application. The cause could lie in a local device, campus network, cloud service, access provider, identity platform or application itself. Troubleshooting is more effective when teams can compare evidence across these layers and rapidly determine who is responsible for the next step.

Measure the service outcome, not just network activity

A useful monitoring framework combines the technical and operational measures appropriate to each critical service. Technical measures may include path availability, delay, packet loss, route changes, application response and relevant access-control events. Operational measures may include time to identify a fault domain, time to restore service, recurrence of incidents, quality of escalation and whether critical work resumed without data loss or unsafe interruption.

Not every service needs the same threshold. Large, scheduled research transfers may depend on predictable throughput and integrity checks; an interactive application may depend on stable response times; a manufacturing process may require locally controlled functionality if the wide-area connection fails. Teams should define measures with the relevant service owner rather than apply one universal performance objective to all facilities.

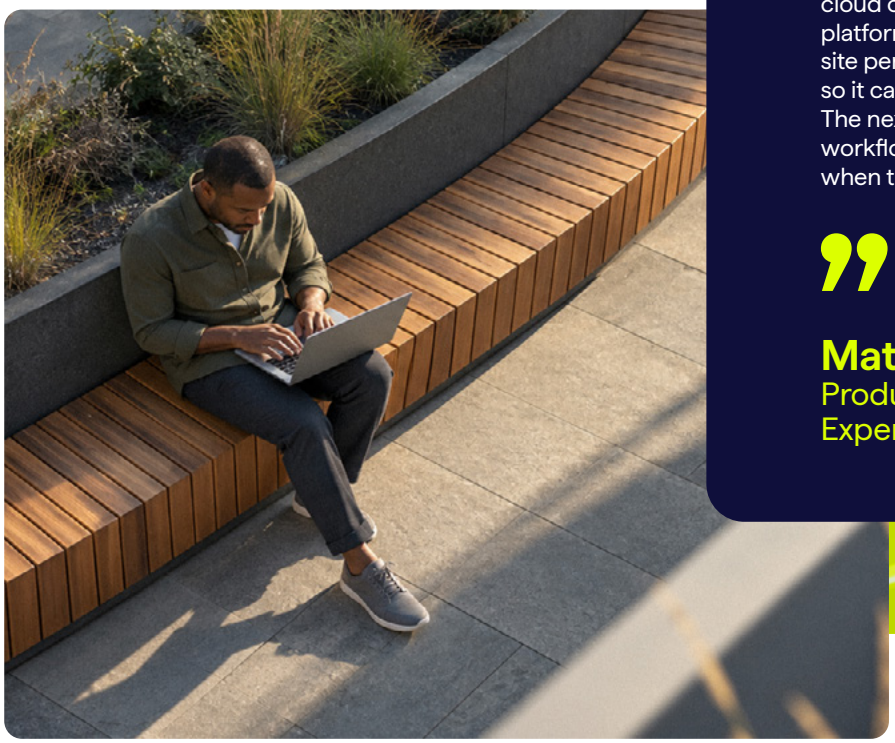
The ISPE GAMP 5 guidance helps frame the importance of systems being fit for intended use in regulated settings. Its focus is not network observability, but it reinforces an essential principle: evidence must be related to the intended function of the system. A network dashboard should likewise contribute to demonstrating that the service supporting a critical workflow is operating as required.

Turn incident diagnosis and recovery into a learning process

Resilience assurance also depends on what happens after an incident. Teams should document the affected service, the fault domain, recovery steps, partner handovers and the evidence used to confirm normal or acceptable operation. If a circuit is restored but an application remains unavailable, the incident should not be considered resolved merely because the network provider has closed its ticket.

Testing should cover realistic multi-component failures. An alternate route may depend on the same building entry point, regional carrier or shared identity service as the primary route. A cloud-based service may be reachable but inaccessible because an authentication dependency failed. Rehearsals can reveal those shared points of failure before an actual disruption occurs.

The aim is not to centralize every operational decision. It is to create consistent evidence that helps the right scientific, IT, engineering, security and supplier teams coordinate their response. Where the evidence is incomplete, a defined escalation process is preferable to automated assumptions about which component has failed.



Strategic insight

Network observability becomes operational assurance when it links service performance, incident causes and recovery evidence to the activities that matter across the pharmaceutical value chain.

For life-sciences organizations, this means combining cross-provider telemetry with a clear understanding of critical workflows and accountable decision-making. Independent visibility tools can support diagnosis and prioritization, but they should be judged by their contribution to restoring research, manufacturing and business services rather than the volume of data they collect.

Once performance information becomes dependable and actionable, organizations can explore more intelligent network operations while retaining the safeguards required for sensitive environments.

Expereo perspective:

Observability should end arguments, not start them

A green dashboard means very little to a scientist who can't open the results they need. Good observability shortens the argument about where the fault sits: device, campus, carrier, cloud or application. That's why the Expereo platform puts service status, open cases and site performance in one view, by portal or API, so it can feed the tools teams already use. The next step is tying that evidence to the workflow it supports, so a ticket closes when the work has resumed.

Matthew Lea
Product Development Director, Expereo



Theme 5:
Building intelligent resilience without compromising control

AI and edge computing may improve responsiveness, but maturity depends on trustworthy information and well-governed interventions.

Life-sciences organizations are exploring a wide range of AI applications, from research analysis to operational forecasting. Network operations represent a narrower set of use cases: identifying abnormal performance, prioritizing alerts, suggesting likely fault domains and supporting decisions about routing or remediation. Those activities involve different information, expertise and controls from AI in drug discovery or manufacturing analytics. Adoption figures from one domain should not be used as proof of adoption in another.

A sensible initial use case might be correlating related alerts from multiple providers or identifying a recurring degradation pattern. Other applications include suggesting the likely location of a fault and improving how information is presented to the responsible engineer. These capabilities can reduce manual work if the underlying data are accurate, but inaccurate telemetry or unclear ownership can make even a plausible recommendation misleading.

AI-assisted decisions should therefore be evaluated against practical outcomes: diagnostic accuracy, false positives, time to identify root cause, restoration quality, the ability to explain recommendations and the absence of unacceptable operational side effects. A pilot that produces more alerts without improving decisions is not evidence of resilience maturity.

Separate network AI pilots from operational deployment

Our analysis classified 53% of modeled discussions as describing pilot use cases for AI-assisted pharmaceutical network resilience and 47% as not yet using AI for that purpose. The classifications do not establish deployment scale, commercial readiness or realized performance improvements. They indicate interest in exploration, while underlining the importance of distinguishing experiments from routine operational capability.

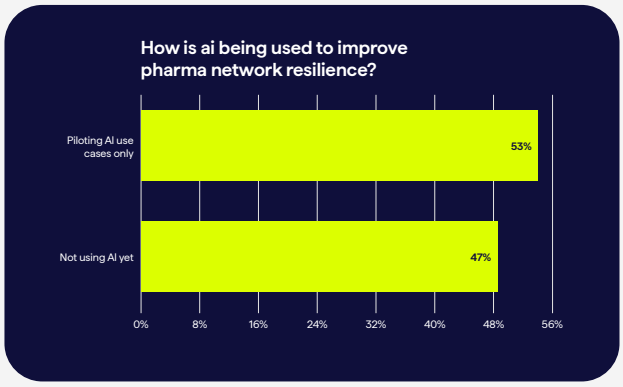


Figure 3. AI use specifically for network resilience





Edge computing is an architectural choice, not a resilience guarantee

The research also classified **65% of opinions** as describing non-use of edge computing while treating it as essential, another **15%** as non-use while regarding it as important, and **21%** as referring to edge computing used at manufacturing sites and viewed as essential. The reported categories total 101% after rounding. They are directional classifications of perceived relevance and use, not an audited deployment survey.

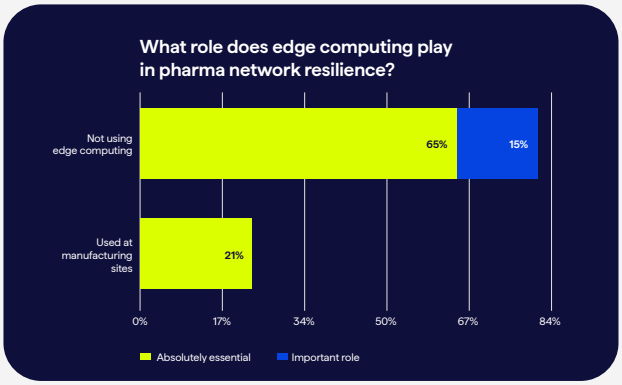


Figure 4. Edge-computing readiness and perceived importance.

Edge computing can help process some information closer to an instrument, facility or production system, potentially limiting dependency on a distant service for selected functions. However, it can also introduce more sites, software components, maintenance responsibilities and data-synchronization pathways. It should be considered only after the required workload, local autonomy, data-handling rules and recovery process are clear.

For a manufacturing environment, the key question is which services must continue locally when wider connectivity is degraded, and how local and central systems will reconcile information after restoration. For a research site, it may be whether a local analysis capability helps maintain a time-sensitive workflow without compromising access control or data quality. These are different decisions that cannot be settled by an edge adoption percentage.

Keep engineering, data integrity and governance in the loop

Intelligent operations require accurate inventories, reliable performance data and clear service ownership. Before network automation changes a production-critical path, teams should determine what the change could affect, what requires human approval and how an unexpected outcome can be reversed. The same discipline applies to AI-assisted diagnosis, where a model's confidence or persuasive explanation should not be mistaken for verified causality.

The NIST AI Risk Management Framework provides a general, voluntary foundation through its Govern, Map, Measure and Manage functions. It is not a pharmaceutical-specific regulatory standard. Alongside risk-based good practice such as ISPE GAMP 5, it helps explain why teams should define scope, testing, oversight and ongoing performance review before more consequential automation is allowed.

Where regulated systems or records may be affected, changes should be assessed with the relevant quality and process owners. A suitable progression begins with advisory tools and supervised recommendations, then selectively introduces bounded automation once the organization can demonstrate the benefit and manage the risk. This protects the distinction between improving network operations and claiming that an AI system can independently make validated scientific or product-quality decisions.

Strategic insight

Intelligent network resilience should be demonstrated through more dependable services, better operational decisions and controlled recovery, not by the number of AI or edge technologies deployed.

For pharmaceutical leaders, readiness depends on trusted data, clear responsibilities, fit-for-purpose architecture and meaningful measures of success. AI and edge computing may help reduce avoidable disruption, but only when introduced around specific service needs with appropriate engineering and quality oversight.

Across the five themes, one requirement is consistent: the network must be understood, measured and governed in the context of the scientific and operational value it enables. The next step is turning these principles into practical priorities for a global life-sciences operating model.



Expereo perspective:

AI earns its place through unglamorous wins

In pharmaceutical operations, the challenge is introducing automation while keeping the supported process under control. AI can help engineers identify related faults and detect declining network performance. Permission to make changes needs tighter limits. Automatic routing within tested boundaries is different from a new configuration change. The evidence must show what changed, which systems were affected and whether the process still operates as intended.

Julian Skeels
Chief Digital Officer,
Expereo



Summary:

Five priorities for the next era of life-sciences connectivity

Five connected priorities emerge from the research, highlighting the capabilities life-sciences organizations need to support discovery, manufacturing and delivery across distributed networks and partners.



1 Map critical workflows and their digital dependencies

Begin with the scientific, quality and business activities that matter most. Identify the sites, applications, data movements, network paths and external partners on which they depend. Agree which processes can operate locally, which require continuous connectivity and what acceptable recovery looks like. Use quality-risk principles to prioritize assurance effort rather than aiming for identical controls everywhere.

2 Extend resilience plans to laboratories and distributed teams

Bring R&D facilities, remote specialists and partner workflows into the same continuity assessment as core offices and production operations. Validate the coverage of critical systems, recovery procedures and data exchanges through realistic scenarios. Use the results to close specific gaps rather than treating a backup link as proof that a laboratory can continue its work.



3 Coordinate providers and services across the global estate

Apply repeatable standards for service requirements, documentation, ownership and escalation across regions and providers. Retain local connectivity flexibility where justified by availability, security or site conditions. Assess managed networking solutions through evidence of service delivery and restoration, not a technology deployment label alone.

4 Use observability to prove service performance and recovery

Connect network monitoring with the applications and processes it supports. Agree service-specific performance baselines, incident attribution and post-restoration checks. Make it clear when a fault originates in access, cloud, security, application or third-party infrastructure, and ensure that the responsible team can act on the evidence.

5 Introduce AI and edge capabilities through controlled use cases

Prioritize use cases where reliable data, tested dependencies and accountable ownership already exist. Start with decision support and defined local processing needs before expanding automation. Assess benefit through fewer recurring disruptions, faster and safer recovery, reliable data handling and measurable improvements in service quality.

Together, these priorities provide a practical basis for assessing life-sciences network resilience and deciding where targeted improvements could have the greatest effect on operational confidence.

Life Sciences Network Resilience Scorecard

A practical, qualitative assessment of the capabilities behind scientific and operational continuity.

The six-dimension scorecard translates the themes into a structured discussion for CIOs, global network leaders, research IT teams, quality stakeholders and service owners. It is an editorial self-assessment, not a survey-based maturity benchmark. Scores should reflect demonstrable current practice, not a roadmap or a vendor's capability claims.

Dimension	Developing	Established	Advanced
1. Critical-service dependencies	Network inventories are site-based; links to scientific or operational processes are unclear.	Critical applications, data paths and external dependencies are documented and owned.	Dependency evidence informs risk reviews, scenario tests and service improvements across the lifecycle.
2. Laboratory and remote coverage	Continuity plans concentrate on core offices; lab and distributed workflows are not assessed consistently.	Priority labs, teams and partners have documented recovery arrangements and periodic tests.	Coverage is revalidated after change; recovery is demonstrated across local and external services.
3. Network and application visibility	Teams see circuit or device health but cannot readily explain application impact.	Shared baselines and incident records support diagnosis of critical services and fault domains.	Cross-provider telemetry and service context support predictive action and accountable recovery.
4. Global provider coordination	Carrier, cloud and support relationships are documented separately; escalations are inconsistent.	Named owners, service records and common escalation processes are maintained across regions.	Coordinated service assurance and recovery work effectively across multiple providers and sites.
5. Security and recovery governance	Access and changes are managed locally; impact on regulated workflows is poorly understood.	Appropriate owners approve changes, test recovery and retain required operational evidence.	Risk-based controls, quality oversight and recovery learning are integrated into routine operations.
6. Intelligent operations readiness	AI ideas and edge plans lack trusted telemetry, business cases or clear operating limits.	Selected use cases have reliable data, evaluation criteria and human oversight.	Governed interventions show repeatable improvements in service quality, response and resilience.

Framework note: This is a qualitative discussion tool derived from the report themes, not a statistically validated benchmark. Classify demonstrated practice, not planned capability.



From assessment to action

A scorecard creates value when it leads to decisions. Organizations should begin with the critical services and locations where improved assurance could materially reduce scientific, operational or business risk. The appropriate action may be a better laboratory dependency map, more effective carrier escalation, a tested recovery route or clearer evidence that regulated data flows can resume correctly after disruption.

A practical first cycle has three steps:

- **Prioritize critical services.** Agree with research, manufacturing, quality and business owners which workloads and data exchanges warrant the greatest resilience attention.
- **Establish evidence and recovery expectations.** Set service baselines, test plausible failure scenarios and document how normal or acceptable operations will be verified after restoration.
- **Assign owners and review improvements.** Clarify the responsibilities of central IT, local teams, security, quality and external partners, then reassess after material changes or incidents.

Strategic outlook: From connected sites to assured science

The next stage of digital life sciences will create more interdependence between research, manufacturing, data platforms and global supply networks. Advanced analytics, connected equipment and outsourced specialisms can improve capability, but they also increase the importance of dependable information flows, transparent responsibilities and workable alternatives when a component fails. A faster network cannot by itself resolve all these dependencies.

There is no universal architecture for every laboratory, production plant or distribution center. The organizations best positioned to strengthen resilience will be those that define critical outcomes clearly, link performance evidence to the activities it supports and coordinate incident response across facilities and external providers. They will distinguish the need for robust global connectivity from the separate responsibilities of regulated applications, manufacturing systems and quality assurance.

That distinction should also change how organizations evaluate providers. Buyers should ask which components of a critical service a partner can actually observe, which incidents it can diagnose and resolve, and where application, cloud, local systems or other carriers remain outside its direct control. Clear boundaries, named escalation owners and a credible recovery process are more useful than a promise of end-to-end control that cannot be demonstrated.

Progress should be visible in operational evidence: fewer unresolved cross-provider incidents, clearer service dependencies, faster identification of fault domains, successful recovery exercises and greater confidence that important workflows can resume safely after disruption. These measures create a more meaningful basis for investment than technology deployment counts alone.

For Expereo, the relevant discussion is how a global managed connectivity partner can support cross-site service visibility, coordinate diverse access providers, improve network operations and help organizations respond more consistently when service conditions change. Any claim about product capabilities or customer outcomes should be validated through SME review and evidence before publication.

The future of life-sciences connectivity is not simply more connected sites. It is confidence that critical work can continue, recover and improve from discovery through to delivery.

Closing perspective

Every handoff is a dependency someone must own

In life sciences operations, restoring a connection is only part of recovery. Teams also need to establish that records are complete and reliable enough to support quality decisions. A connection can be working again while a batch remains on hold. At Expereo, we coordinate connectivity across providers and make network performance and incidents visible. That gives customers clearer information about the disruption while their quality and production teams manage the wider recovery.

Julian Skeels
Chief Digital Officer,
Expereo



Continue the conversation

The scorecard provides a starting point for identifying where better network visibility, coordinated service management or more resilient cross-site connectivity could make the greatest difference. To explore global connectivity and managed networking priorities, visit Expereo

[Nominated Expereo contact: full name and job title]

[LinkedIn profile, if required]

[Contact email, if required]

Visit Expereo