Measuring Confidence in Cloud-Hosted Applications

Nov 24, 2026 · @Steve Carroll

Community banks and credit unions need a way to measure how much confidence they have in each cloud-hosted application their vendors provide, and to show whether that confidence is rising or falling. Two outages this month made the case. On November 12, Microsoft 365 went down for nearly 24 hours. The next afternoon, the FAA stopped every departure in the country. Neither was a cyberattack. Both began with routine changes made by the people responsible for running those systems.

This article proposes a simple method: a confidence score from 0 to 100, built from the due diligence evidence an institution already collects, and a direction indicator that flags whether the picture is getting better or worse.

Two outages in two days

Microsoft 365, November 12 and 13. The outage started at 11:20 a.m. Eastern on November 12 and lasted 23 hours and 50 minutes (365Fanatic summary of Microsoft's incident report). Exchange Online took the worst of it. Teams, SharePoint, Power Apps, Power BI, Intune and Defender were also affected. According to Microsoft's preliminary report, three ordinary conditions lined up:

- A defect in a gateway fix that had run without trouble for more than three months.
- Extra load after Teams failed over to the same gateway, which is how failover is supposed to work.
- About 14% of the gateway's servers already offline from an unrelated problem.

At the low point, more than 80% of the gateway servers stopped responding. The partitions that should have kept the failure in one region did not hold. Microsoft's test labs ran on older hardware with fewer processor cores, so the problem never showed up in testing.

FAA air traffic control, November 13. At 3:54 p.m. Eastern, the FAA ordered a nationwide ground stop that lasted about four and a half hours (Wikipedia). Radio and radar feeds failed at 17 of the 22 regional centers that manage en route traffic. Nearly 8,000 flights were canceled that day, with more cancellations over the following two days. Investigators are looking at new routers installed during a copper-to-fiber upgrade of the

FAA's telecommunications network. A contractor owns, operates and maintains that network, and a different company makes the routers. In other words, this was a third-party and fourth-party event.

What Microsoft's CEO said next. At the New York Times DealBook Summit, Satya Nadella warned that more outages are coming (New York Post via Finwire). His reasoning: AI tools now find software flaws faster than before, every flaw found has to be patched, and each patch carries its own risk. He described much of the trouble as "old infrastructure with new patches and instability." He also called Microsoft's outage a perfect storm and said the company should have caught it in testing.

The pattern is the same in all three accounts. Change is constant, the systems are interconnected, and a provider with good controls can still have a very bad day. An institution's job is to know how much it is relying on each provider, how sure it is of that provider, and whether that confidence still holds.

Why examiners are likely to ask for this

The 2026 proposal moves third-party risk away from fixed checklists and toward judgment, and an institution has to be able to show how it reached that judgment. On September 11, 2026, the Federal Reserve, OCC, FDIC and NCUA jointly proposed guidance that would replace the 2023 interagency guidance (Federal Register). This is the first time NCUA has joined, so banks and credit unions would work from the same framework. The comment period closed on November 16, 2026.

According to Davis Wright Tremaine's summary, the proposal makes four changes that bear directly on confidence scoring:

- It drops the "critical activity" label. Instead, an institution weighs how much harm a relationship could cause and how likely that harm is.
- It accepts that some residual risk can't be avoided, and lets an institution make an informed decision to accept it.
- It replaces the 2023 list of more than 15 monitoring factors with principles each institution tailors to its own size and risk profile.
- It says examiners will give due consideration to an institution's reasonable decisions.

The last point is the one that matters for exams. A decision gets that consideration only if it can be shown to be reasonable. When a vendor's controls lower the likelihood of harm, the examiner's next question is what evidence supports that, and how current it is. A

confidence score with documented evidence levels answers that question directly. A trend indicator answers the follow-up: what the institution did when the evidence changed.

The proposal could still change before it becomes final. Even so, the direction is unlikely to reverse. Examiners have asked how institutions oversee their vendors for years, and the outages above will keep operational resilience on their list.

Know where the system actually runs

Knowing that a vendor's system is "in the cloud" is not enough. A risk manager also needs to know whose cloud it runs on, in which regions, and how many of the institution's other vendors depend on that same platform. The bank or credit union contracts with the vendor, which is the third party. The vendor rents computing capacity from a cloud platform, which is a fourth party. The institution has no contract with that fourth party, but its critical functions still depend on it.

Both November outages showed how this works. Every vendor whose product relied on Microsoft 365 or the services behind it went down along with Microsoft. The FAA's network failed after work by the contractor that runs it, using equipment from yet another company.

A handful of companies host most of the cloud workloads that vendors run on. In the third quarter of 2026, the top three held about 61% of worldwide spending on cloud infrastructure (Synergy Research Group, via DCD):

Cloud platform	Share of worldwide cloud infrastructure, Q3 2026	Where its audit reports are kept
Amazon Web Services (AWS)	26%	AWS Artifact
Microsoft Azure	19%	Microsoft Service Trust Portal
Google Cloud	16%	Google Compliance Reports Manager
Oracle Cloud Infrastructure	Smaller share; common for core and enterprise software	Compliance Documents in the Oracle Cloud Console (Oracle)

What a risk manager can learn about a fourth party

The large cloud platforms won't fill out a bank's questionnaire or sign its contract. Even so, they publish more than most third parties do:

- **Independent audit reports.** All four publish SOC 1 and SOC 2 reports, ISO certificates and PCI attestations through the portals listed above. Oracle also posts bridge letters for the gaps between SOC reports (Oracle). Some portals require an account; when they do, ask the vendor to supply the reports.
- **Shared responsibility.** Each platform publishes which controls it covers and which belong to its customer, here the vendor. Compare that with the vendor's own SOC report to make sure nothing falls between them.
- **Outage history.** Each platform keeps a public status page and posts reviews after major incidents. Microsoft released its final report on the November outage on November 20.
- **Financial condition.** All four are units of public companies that report results every quarter.
- **Regions.** Each platform publishes where its data center regions are. The vendor has to tell you which ones your data and your recovery copy use.

What to ask the vendor

- Which cloud platform, and which regions, host our production systems and our backups?
- Do production and recovery run in different regions, or only in different data centers within one region?
- Does your SOC 2 report include the cloud platform's controls, or carve them out? If it carves them out, will you provide the platform's report and show how you meet its complementary controls?
- Which other subservice providers do you rely on, and will you notify us before you change platform or region?

Then look across the whole vendor list. If the core processor, online banking platform and loan system all run in the same region of the same cloud platform, one bad day at that platform becomes three vendor outages at once. That concentration belongs in the risk assessment even when each vendor scores well on its own.

The third parties that never send an invoice

Some of an institution's most important third parties never appear on its vendor list. There's no negotiated contract and no invoice, so the contract file and the accounts payable cross-check both miss them. The interagency guidance still covers them. The 2023 guidance says a third-party relationship can exist without a contract or payment (Federal Reserve).

Most of these relationships run under some governing document, such as operating circulars, a membership agreement or network rules. Nobody negotiates it, and nobody files it with the vendor contracts. Fees, if any, come out as a settlement debit or an account analysis charge. In our consulting work, these relationships most often come to light during the business impact analysis. A department manager describes how the work gets done, and that is the first time the dependency is written down.

Type	Examples
Payment and settlement networks	Federal Reserve services (Fedwire, FedACH, FedNow, check services); the Federal Home Loan Bank; correspondent banks and, for credit unions, corporate credit unions; The Clearing House ACH and RTP networks; card, ATM and shared branching networks
Government and agency systems	FinCEN BSA E-Filing; the OFAC sanctions list; regulatory call report filing systems; IRS and Treasury payment systems; SBA E-Tran; Fannie Mae, Freddie Mac and MERS
Free, bundled or informal arrangements	Free online tools staff rely on; internet, generator, HVAC and access control that come with a building lease; reciprocal backup-site agreements with another institution
Card-paid subscriptions	Online services paid on a corporate card, which have terms of service but never pass through accounts payable

How to find them

- Ask each department during the BIA: what outside organization would stop your work if it went down?

- Review the general ledger for settlement debits and account analysis charges.
- Review corporate card statements for recurring subscriptions.
- Use firewall logs or a discovery tool to find online services that staff use.

Many of these relationships call for little due diligence. No one needs to review the Federal Reserve's finances. Their impact on continuity can still be high: if Fedwire is unavailable, the wire room needs a plan. These relationships belong in the inventory, with a note on how each was found and what it is based on, so they can be tied to the business functions that depend on them.

The confidence score

Each vendor gets a score from 0 to 100, built from eight areas of due diligence. Each area is rated on two questions: how strong is the evidence, and what did it show.

How strong is the evidence (0 to 4)

- **0:** Nothing received.
- **1:** The vendor's own word, such as a questionnaire or self-attestation.
- **2:** Documented, such as a policy, a contract clause or a written commitment.
- **3:** Independently tested, such as a SOC 2 Type II report, ISO 27001 certification or a third-party penetration test.
- **4:** Independently tested, and seen working by the institution. Examples are taking part in the vendor's disaster recovery test or pulling its own access logs.

What the evidence showed (a multiplier)

- Clean: 1.0
- Minor exceptions: 0.75
- Significant exceptions or gaps: 0.5
- A material issue that hasn't been fixed: 0.25

Points for each area:

Points = Weight × (Evidence ÷ 4) × Multiplier

Area	What it covers	Weight
Resilience	RTO and RPO compared with the institution's BIA, failover, backups, DR test results, outage history	20
Shared responsibility	Which controls belong to the vendor, the cloud platform, and the institution	15
Data protection	Data location, encryption, who holds the keys, tenant separation, return and destruction of data	15
Access and monitoring	MFA, privileged access, logging, and the institution's own access to its logs	15
Hosting model and fourth parties	Service model, cloud platform and regions, subservice providers	10
Incident notification	Notice time frames that meet the computer-security incident notification rule	10
Contract terms	Right to audit, data ownership, exit assistance, notice of changes	10
Vendor viability	Financial condition, insurance, concentration	5

Two rules keep the score honest:

- **Resilience is checked against the BIA.** If the vendor's recovery time is longer than the institution's own recovery target for any function that depends on it, the multiplier is no higher than 0.5. This applies even when the SOC report is clean.
- **Weakest-link cap.** If resilience, data protection or shared responsibility scores below 40% of its weight, the overall score can't go above 49. Strength in other areas can't hide a gap in a core one.

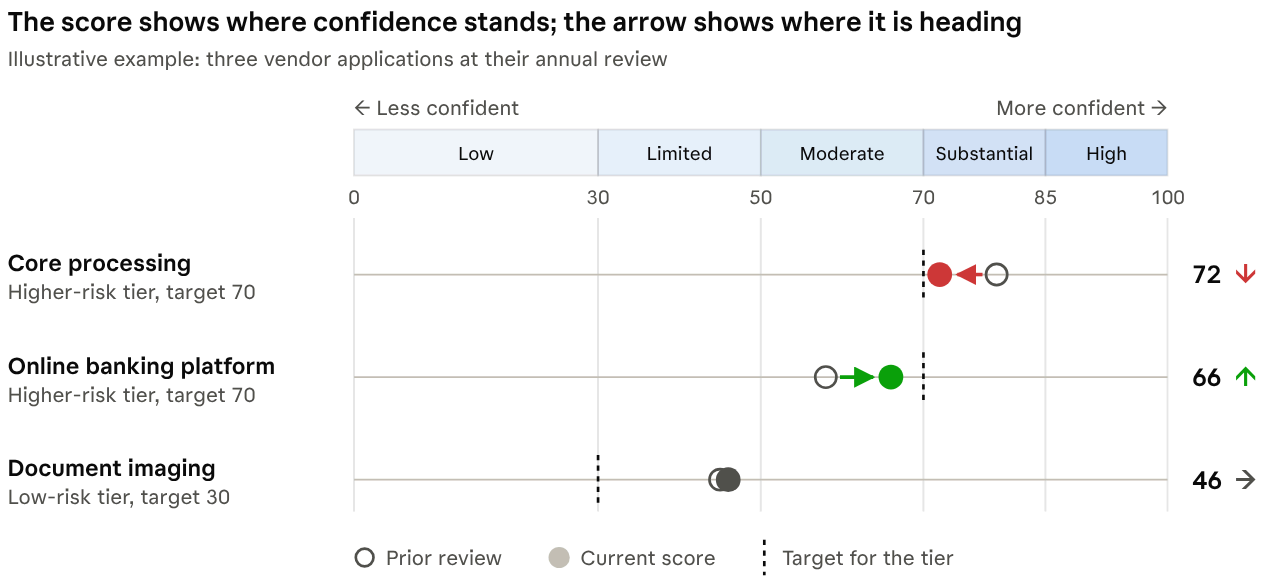
Score	Confidence level
85 to 100	High
70 to 84	Substantial
50 to 69	Moderate

Score	Confidence level
30 to 49	Limited
0 to 29	Low

The Microsoft outage shows why evidence strength is scored separately. A clean SOC 2 report would not have predicted that event. The deciding question is whether the institution knows what happens to its own critical functions when that vendor goes down, and has tested it.

Which way it is heading

The score shows where confidence stands today. The arrow shows whether it is improving, stable or declining, and it is often the more useful of the two.



Mock-up: confidence score, prior review and direction indicator for three sample vendors

In this example, the core processor still clears its target at 72. It has dropped 7 points since the last review because its SOC report expires in 60 days and no bridge letter is on file, so it is the one to act on first. The online banking platform is below its target, but the arrow shows remediation is working. Document imaging is comfortably above its lower target and stable.

How the arrow is set

- **Declining (↓)** when the score has dropped 5 or more points since the last review, or when any of these happens: the SOC report is more than 12 months old with no bridge letter; the auditor gave a qualified opinion; a new subservice provider hasn't been assessed; there was a material outage or security incident; or there is adverse news about the vendor's finances.
- **Improving (↑)** when the score has risen 5 or more points, or when open findings have fixes that will be verified within 90 days.
- **Stable (→)** in all other cases.

If both a declining and an improving condition apply, the downward arrow wins.

What score each tier needs

The proposed guidance asks institutions to weigh how much harm a relationship could cause. That weighing sets the vendor's risk tier, and the tier sets the confidence the institution needs:

Risk tier	Target score
Higher risk	70 or above
Moderate risk	50 or above
Low risk	30 or above

A score below the target for its tier produces a finding with a follow-up task. Together, the gap to target and the arrow show which vendors need attention first.

Worth doing however the rules turn out

Whatever form the final guidance takes, a confidence score gives management something it doesn't have today: one consistent way to compare vendors and to see when a vendor needs attention. Here is why it pays off on its own:

- **It focuses limited staff time.** Most community institutions have one or two people handling vendor management. A score below its target, or a downward arrow, tells them where to spend the next hour.
- **It ties vendor risk to the BIA.** The resilience check compares each vendor's recovery commitments with the recovery times the institution already set for its business functions. That turns a vendor review into a continuity conversation.

- **It catches decline before an outage does.** An expired SOC report, a new subservice provider or a string of incidents moves the arrow down before anything breaks.
- **It gives the board a clear picture.** A one-page list of critical vendors, each with a score, an arrow and a target, shows where the institution stands far better than a stack of due diligence files.
- **It shows judgment over time.** Asked why the institution kept a vendor after an incident, management can point to the score, the evidence and the actions taken.

The outages of November 12 and 13 won't be the last. Microsoft's own CEO expects more. An institution can't prevent a provider's bad day. It can know ahead of time which providers it depends on most, how well it understands them, and whether that understanding still holds.