Vendor Cyber Risk Assessment Toolkit

A Practical Resilience Resource for Long-Term Care Organizations Navigating the Risks of a Digitally Connected Ecosystem

INSURICA HEALTHCARE

Table of Contents

Section 1: Why Vendor Cyber Risk Matters.....1
Section 2: Vendor Risk Assessment Checklist.....2-3
Section 3: Red Flag Indicators.....4-5
Section 4: Internal Vendor Review Process.....6-7
Section 5: Navigating Pushback & Next Steps.....9

As long-term care organizations grow more dependent on cloud based platforms, outsourced IT providers, and digital vendor ecosystems, understanding and managing third party cyber risk has become essential.

This toolkit is designed to help leaders systematically evaluate the cyber readiness, resiliency, and contractual strength of their vendors to reduce the risk of disruption, data exposure, and regulatory fallout.

Section 1: Why Vendor Cyber Risk Matters

Vendors often serve as the weakest link in an organization's cybersecurity chain. A breach at your billing platform, pharmacy partner, or EHR provider can expose sensitive data, disrupt operations, and damage trust, even if your internal systems are well secured. With many vendors leveraging shared infrastructure like AWS or Microsoft Azure, the potential for cascading failures is real. Regulatory agencies increasingly expect due diligence and documentation of vendor oversight.

KEY RISKS:

- Lack of encryption or endpoint protection
- Weak internal access controls
- Failure to meet notification or recovery timeframes after an incident
- Inflexible or one sided contracts
- Lack of auditability or transparency
- No protocols for planned downtime or system upgrades
- Unclear or absent incident response plans
- No documentation on subcontractor or cloud platform dependencies (e.g., AWS, Azure)
- Limited cyber awareness among frontline or non-IT staff
- Failure to conduct regular internal cybersecurity reviews or tabletop exercises

Tips for Applying This Toolkit:

- Start with your highest risk vendors. Focus first on those with access to PHI, financial data, or essential systems (e.g., EHR, billing, pharmacy).
- Don't rely on reputation. Well known vendors aren't immune, assess them like any other.
- Use this toolkit as a conversation starter. Sharing your expectations with vendors can prompt better alignment, not just evaluation.
- Document everything. Regulators and insurers increasingly expect proof of oversight, not just verbal assurance.
- Schedule reviews annually or after major changes. Re-evaluate vendors after software migrations, M&A events, or security incidents.

Section 2: Vendor Assessment Checklist

This checklist is designed to help your team assess and compare the cyber risk posture of your critical vendors. It focuses on clear, practical indicators of readiness, transparency, and risk exposure, without overcomplicating the process.

Use it to:

- Identify vendor vulnerabilities before they create downstream risks
- Track and compare performance across multiple vendors
- Justify follow-up actions, contract revisions, or leadership decisions
- Document due diligence for auditors, insurers, and regulators

HOW TO USE THE CHECKLIST

Score Each Item

Assign a value from 0–3:

0 = Not Met / Unknown

1 = Minimal Evidence or Incomplete

2 = Partially Meets Expectation

3 = Fully Meets Expectation

Add Total Score.

The maximum possible score reflects the number of items included (e.g., 13 items = 39 points). Use the risk tier guidance at the bottom of the page to interpret the vendor's overall posture.

Compare Across Vendors

Use the same checklist across your top vendors, especially those with access to sensitive data, cloud dependencies, or operationally critical roles, to create a simple snapshot of where risks exist and what needs attention.

Document the Process

Keep a record of assessment dates, who participated, vendor responses, and any follow-up actions taken. This can support compliance and insurance alignment.

Tailor to Your Organization

You're encouraged to:

- Add or remove checklist items based on your vendor type (e.g., EHR vs. cloud backup)
- Invite participation from IT, compliance, and operational leads to ensure a well-rounded review
- Adapt this into your broader vendor due diligence or procurement processes

Even if your organization is early in developing a formal review process, this checklist creates a strong foundation for better vendor conversations and more resilient partnerships.

See example of checklist / assessment below:

Vendor Scoring Table

Assessment Item	Vendor A	Vendor B	Vendor C	Notes / Evidence / Follow-up Needed
Written cyber policies & responsible party named				
MFA for admin accounts				
Encryption (data in transit & at rest)				
Backup & disaster recovery protocols				
Defined breach response timelines in contract				

Need the Full, Downloadable Checklist?

This toolkit includes a preview, shown above, the full assessment includes more areas to focus on.

If you'd like the full downloadable version, help tailoring it to your vendor types, or guidance building a formal due diligence process reach out to Drew Colwell at INSURICA.

Drew.Colwell@INSURICA.com 406-991-1727 LinkedIn.com/drewcolwell

Section 3: Red Flag Indicators

Even when a vendor appears reputable, certain signs may indicate elevated cyber risk. These red flags don't always mean you should end a relationship, but they do warrant deeper scrutiny, documentation, and internal discussion. Knowing what to look for can help you catch issues early and make more informed decisions.

Refusal to provide documentation or cyber insurance proof

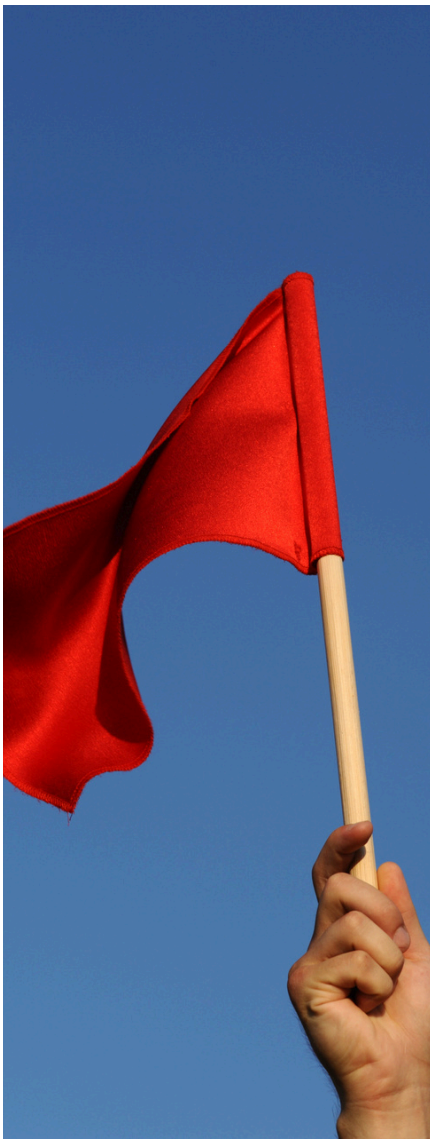
- Lack of transparency may signal weak internal practices or a resistance to oversight. Even if the vendor is widely used, this should raise serious questions about risk exposure.

Lack of contractual SLAs for breach response

- Without guaranteed timelines or notification clauses, your organization may face longer recovery times and unclear accountability in the event of a breach.

No clearly defined escalation plan or emergency contact process

- Vendors without an emergency protocol may be unprepared to support you when incidents occur. This increases confusion and delays in critical moments.



Over-reliance on verbal assurances without supporting documentation

- If a vendor frequently says “trust us” but offers no evidence, it limits your ability to demonstrate due diligence and protect yourself in case of future fallout.

Resistance to security audits or outside assessments

- Refusal to allow third-party validation, even at a high level, may indicate a lack of preparedness, outdated controls, or unwillingness to improve.

Tips:

- Treat any red flag as a signal to pause and ask more questions.
- Flag the concern in your vendor tracker and elevate internally if unresolved.
- Use red flags to prioritize which vendors should be reviewed more frequently.

Even if a vendor won’t share detailed documentation, you can still ask, “Can you walk us through how you would respond to an incident affecting our data?”

Section 4: Internal Vendor Review Process

Vendor risk doesn't start and stop with onboarding. Without a consistent internal process, even well meaning diligence efforts can become scattered, siloed, or reactive. A repeatable system ensures that key questions are asked, issues are documented, and strategic decisions are aligned with your organization's risk tolerance, compliance needs, and operational goals.

KEY PROCESS RECOMMENDATIONS:

Categorize vendors by criticality and data exposure
Identify which vendors have access to sensitive resident data, affect patient care, or impact daily operations. Tier them into levels (e.g., critical, moderate, low) to guide frequency and depth of reviews.

Centralize tracking and documentation
Use a shared tracker or scorecard to log vendor reviews, red flags, contractual terms, cyber insurance status, and contact information. This allows continuity even if leadership or IT personnel change.

Require annual cybersecurity attestations or risk reviews
Don't let vendor risk fade into the background. Require vendors to re-attest to their security practices annually or re-submit documentation — especially when contracts renew**.**

Coordinate with legal, compliance, and insurance
Your legal team can flag liability traps. Your insurance broker can check whether vendors meet requirements of your cyber policy. Internal alignment helps avoid gaps.

Integrate into your broader risk and procurement strategy
Vendor reviews shouldn't be a standalone effort. Align them with IT upgrades, insurance renewal timelines, strategic sourcing, and emergency preparedness planning.

Roles to Involve:

- Executive leadership
- Compliance or quality officer
- IT manager or consultant
- Risk manager
- Legal counsel
- Insurance broker

Do You Need a More Formalized Process?
For organizations without a current vendor risk review process, start small. Build a simple quarterly review calendar, assess 1–2 vendors per month, and grow from there. The goal is progress and consistency, not perfection from day one.

Section 5: Navigating Pushback & Next Steps

Even with a solid process and clear questions, many organizations encounter pushback from vendors, especially large or entrenched ones. That doesn't mean the effort is wasted. The true value of a strong vendor cyber strategy is not just in getting answers, it's in documenting the questions, clarifying your expectations, and shifting the culture toward transparency and shared responsibility.

COMMON CHALLENGES YOU MAY FACE:

- "We don't share that information."
- "That's in our standard contract, no exceptions."
- "We're too large to tailor our terms for every client."
- "We've never had another facility ask us this before."

HOW TO STAY STRATEGIC:

Reframe the conversation.

- Ask open ended questions like "Can you walk us through your incident response protocol?" instead of "Will you send us your IRP?"

Ask what they can provide.

- Many vendors have due diligence packets or SOC 2 summaries they share upon request.

Leverage your network.

- If you're not the only organization using a vendor, consider joint advocacy through your association or regional coalition.

Document refusal or delays.

- Even if a vendor declines to participate, keeping records shows due diligence to insurers, surveyors, and your own leadership.

Know when to escalate.

- If a vendor presents unacceptable risk, especially around PHI, financial data, or care delivery, involve leadership or legal to determine next steps.

Final Takeaway

You may not get every answer, but the process itself is a signal, to vendors, regulators, and your own team, that cyber resilience is not optional. By asking better questions, tracking what matters, and knowing when to push, your organization moves from passive consumer to proactive partner.

NEED HELP NAVIGATING THE VENDOR RISK CONVERSATION?

We support long-term care organizations across the U.S. in strengthening their vendor review process, from building internal scorecards to coaching leadership through vendor due diligence. If you'd like to explore how to scale this toolkit into a more formalized strategy or adapt it for high-exposure vendor types (e.g., EHR, pharmacy, MSP), reach out to Drew Colwell at INSURICA.

Broker: Drew Colwell
Phone: 406-991-1727
Email: Drew.Colwell@INSURICA.com

An **Assurex** Global Partner

INSURICA HEALTHCARE