Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/cyber-due-diligence-before-close/

TRANSACTIONS

Pre Close Cyber Due Diligence for Breach Liabilities

An acquirer that examines the target network before close learns what is already inside it, from an undetected intrusion to an undisclosed breach, while there is still time to price it. Put a technical assessment inside the diligence window and tie its findings to the agreement. Call (800) 868-8189 at any hour.

Published September 3, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Why Technical Testing Belongs Alongside the Diligence Questionnaire

In private equity buyouts, strategic corporate acquisitions and venture investments, traditional pre close cyber due diligence often consists of handing the target company IT director a spreadsheet of compliance questions and reviewing their SOC 2 certificate. Technical testing before close is how acquirers look past self reported answers for an active network intrusion, unpatched legacy infrastructure requiring millions of dollars in unbudgeted capital expenditure, or proprietary software built on copyleft open source code that reshapes the target core intellectual property valuation.

Technical Compromise Assessments, Attack Surface Validation and Source Code Audits

Working directly for deal counsel, private equity operating partners and corporate development teams, Global Digital Forensics conducts rapid, deal speed technical due diligence engagements before close. Our specialists test the questionnaire answers directly, performing external attack surface reconnaissance, Active Directory and cloud identity configuration reviews, targeted compromise assessments that look for threat actors inside the target network, and SourceScan software reviews when software IP is driving the transaction multiple. We translate every technical finding into concrete financial terms, quantifying immediate remediation costs, post close integration risks and specific escrow or representation and warranty adjustments for the purchase agreement.

© 2026 Global Digital Forensics, Inc. All rights reserved.

What a Pre Close Assessment Can Establish

A technical diligence engagement produces evidence the deal team can weigh and price. A compromise assessment can show whether the target's endpoints, servers and identity systems hold indicators of current or past intrusion: persistence mechanisms, anomalous scheduled tasks, remote access tools the IT staff did not deploy, mailbox rules that forward outward, privileged accounts no one can explain and sign in patterns from infrastructure that does not belong to the business. An identity and cloud configuration review can show whether multi factor authentication is enforced, whether legacy protocols are open and how many administrators exist. An external attack surface review can show what is exposed to the internet today and whether it is patched.

The assessment reads what the target's systems logged, so we measure the depth of visibility as carefully as the findings. For a target with light endpoint telemetry and short log retention, a quiet result covers a window of weeks, and the report states that window so the deal team weighs the result correctly. A source code review through SourceScan identifies the open source components and licenses inside the product the valuation depends on, and the review extends to the modules that matter most when the secure practice of the target's own engineers is in question. Diligence that states its depth of coverage gives a representation and warranty negotiation solid footing, and our cyber due diligence reports are written to carry that coverage forward into the agreement.

Reading the findings as a deal team member means separating three categories. Some findings describe risk the acquirer can price and fix after close, such as missing multi factor authentication on administrator accounts or unpatched external services, and those belong in the integration budget. Some describe liabilities that already exist, such as evidence of a past intrusion the target did not disclose or regulated data held in violation of a stated policy, and those belong in the representations, the indemnity and possibly the price. Some describe open questions that call for more visibility, and those belong in post close monitoring covenants. We sort findings into those categories explicitly, because sorting lets the deal team give the fixable and the inherited each its proper weight.

Regulatory Clocks That Follow the Target Into the Deal

A public acquirer takes on the target's incidents as its own. Under the Securities and Exchange Commission rules adopted in July 2023, a registrant must disclose a material cybersecurity incident on a current report generally due four business days after determining the incident is material, and must describe its cybersecurity risk management and governance in its annual report. An undiscovered intrusion inside an acquired subsidiary becomes a disclosure question the moment the acquirer's team finds it, with a materiality analysis that now includes the acquirer's own market capitalization. Pre close knowledge changes that analysis, the purchase price and the indemnity structure, which is why deal counsel wants the technical findings before signing rather than after.

State and sector regimes travel with the data. A target holding New York residents' private information carries notification duties under the SHIELD Act, a target holding protected health information carries HIPAA breach notification duties with a 60 day outer limit under 45 CFR 164.404, and a target in the defense supply chain carries DFARS 252.204-7012 reporting duties and the CMMC assessment obligations that the acquirer will have to maintain to keep the contracts. A target that processes payment cards carries PCI DSS obligations

© 2026 Global Digital Forensics, Inc. All rights reserved.

whose current state the acquirer should see in the actual assessment reports. We identify which regimes apply during scoping so the assessment tests the controls those regimes require, and so the deal lawyers can draft the representations around facts rather than categories.

How the Engagement Fits a Deal Timeline

Diligence runs on the deal's calendar, so the engagement is organized to deliver usable findings in stages rather than one report at the end. The first phase works from the data room and interviews: policies, prior assessments, insurance applications, incident history, architecture diagrams and the target IT leadership's own account of the environment. External reconnaissance begins at the same time because it needs no access and often surfaces exposed services, forgotten subdomains and leaked credentials within the first days. Deal counsel receives an early memo on anything that would change the negotiating posture, because a finding delivered before price is agreed carries its full value into the negotiation.

The second phase requires access and is governed by a clean team protocol agreed between the parties. Our engineers deploy or read from endpoint telemetry to sweep for compromise indicators, review Active Directory and cloud identity configuration, examine backup integrity and segmentation, and where software is the asset being acquired run a source code review for security defects and license obligations. Each finding is translated into terms the deal team uses: the remediation cost, the integration risk, the regulatory exposure and the proposed treatment in the agreement, whether an escrow, a specific indemnity, a closing condition or a price adjustment. The final report is the record that supports those terms, and the same team can return after close for the verification work that confirms the target was remediated before networks are joined.

After signing, the assessment's value continues into integration. Before any network connection, directory trust or shared identity is established between acquirer and target, the compromise assessment should be refreshed on the target's environment as it stands at closing, because the diligence sweep may be weeks old by then and the announcement of the sale itself draws attackers to the target. The findings memo becomes the integration team's remediation list, with owners and dates, and the retest record shows the board and the auditors that the risks identified in diligence were actually closed. Acquirers who refresh the sweep before joining networks begin ownership with a dated record of what was found, what was inherited and what was fixed.

Deal Practices That Bring Liabilities Into View

The first practice is reading a certificate for what it covers. A SOC 2 report covers the systems and criteria the target chose, during a period that ended before the deal, so the compromise assessment is what looks at the environment as it stands today. The second is independent testing: our engineers run the tools and read the results, which keeps the evaluation separate from the people whose work is being evaluated. The third is reviewing identity at every target, small ones included, since one unmonitored global administrator with a reused password is the typical entry point for an inherited incident. The fourth is examining software provenance in a technology acquisition, because copyleft obligations inside the product can reshape the valuation.

© 2026 Global Digital Forensics, Inc. All rights reserved.

The fifth practice comes after signing: the compromise assessment is refreshed on the target before networks connect and directories join, so any inherited intrusion is addressed inside the target first. Putting these practices in place is a matter of acting early. Technical diligence belongs in the timeline at the letter of intent stage rather than at confirmatory diligence. The operating partner or corporate development lead secures the target's agreement to a clean team protocol and telemetry access. The target's CIO assembles log exports, asset lists, prior assessment reports and the identity configuration before the engineers arrive. For portfolio owners who manage this repeatedly, our private equity and mergers practice page describes the standing arrangements that make each deal's diligence faster, and our executive cyber risk advisory covers board level reporting on acquired risk.

Put Veteran Forensic and Security Architects on Your Deal Team

Whether your transaction closes in ten days or thirty days, call Global Digital Forensics at (800) 868-8189 to scope an M&A cyber due diligence engagement. The initial consultation is free, and our cyber due diligence service page describes the deliverables a deal team receives.

Findings Sorted the Way a Deal Team Must Read Them

Sorting findings by category gives the fixable and the inherited each its proper weight. This table sorts the kinds of finding a pre close assessment produces by what they mean for the transaction and where each belongs in the agreement. Read it when translating technical results into escrow, indemnity or integration terms. The last column names the treatment, and deal counsel draws the legal conclusion.

Categories of diligence finding, an example of each and where it belongs in the deal.

Category	Example finding	Where it belongs
Priceable and fixable risk	No multi factor on administrator accounts	The integration budget
Inherited liability	Evidence of an undisclosed past intrusion	Representations, indemnity and possibly price
Regulated data exposure	New York private information held against stated policy	Representations drawn around the applicable regime
Open question for monitoring	A quiet result over a short log retention window	A post close monitoring covenant
Software provenance	Copyleft components inside the product	The intellectual property valuation
Post signing exposure	Target environment awaiting a refreshed sweep before networks join	A closing condition and a refreshed compromise sweep

The insurance company examination shows how a staged review of public records followed by an onsite systems examination surfaced inconsistencies beyond what a questionnaire captures, the deal speed scrutiny this guide brings before close.

© 2026 Global Digital Forensics, Inc. All rights reserved.

How to Begin and What Happens on the First Call

Have ready a description of the target, its approximate size in endpoints, servers and cloud tenants, the deal timeline with the signing and closing dates, whether software is the asset being acquired, the regulatory regimes you believe apply and the name of deal counsel. Our engineer asks what access the target has agreed to, whether a clean team protocol exists, what prior assessments and incident history the data room holds and which findings would change the deal for you. You then receive a written scope matched to the diligence window, a staged timing plan that delivers early findings before terms are fixed and a proposal for the assessment and report. The initial consultation is free, and the hotline at (800) 868-8189 is answered 24/7 when a deal moves on a weekend.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: NIST Cybersecurity Framework 2.0, NIST SP 1305 and cybersecurity risk management and incident disclosure rule.

Authorities cited in this guide: SEC press release 2023 139, cybersecurity risk management and incident disclosure rules. Announces the July 2023 rules requiring disclosure of material cybersecurity incidents generally within four business days of the materiality determination, as published by the Commission. 45 CFR 164.404, notification to individuals. States the HIPAA breach notification duty and its 60 calendar day outer limit that a target holding protected health information carries, in the current Code of Federal Regulations text. NIST Cybersecurity Framework 2.0. Provides the Govern, Identify, Protect, Detect, Respond and Recover structure used to organize diligence findings for the deal team, in the final Framework 2.0 publication. New York Attorney General, SHIELD Act. Describes the notification duties that follow a target holding New York residents' private information, as published on the current Attorney General resource page.

FREQUENTLY ASKED

Diligence Timing, Cost and Deal Terms

How long does pre close cyber due diligence take?

It is built to fit the diligence window rather than to set it. The drivers are the size and complexity of the target environment, how quickly the target grants telemetry and configuration access under the clean team protocol, whether source code review is included and how many regulatory regimes apply. External reconnaissance and data room review start immediately and produce early findings. The compromise assessment and identity review follow as soon as access is granted. We deliver in stages so the deal team has what matters before price and terms are fixed.

© 2026 Global Digital Forensics, Inc. All rights reserved.

What does cyber due diligence cost on a deal?

The initial consultation is free and the proposal is scoped to the target and the deal. Cost is driven by the number of endpoints, servers and cloud tenants to be assessed, whether source code review is part of the scope, how many sites or subsidiaries the target operates, the regulatory regimes whose controls must be tested and the depth of reporting the deal team and its lawyers need. For repeat acquirers, a standing arrangement reduces the setup for each transaction.

Can you tell us whether the target has already been breached?

We can tell you whether the systems we examine hold indicators of compromise, past or present, and how deep the visibility was that produced that answer. A target with endpoint telemetry and long log retention gives a strong basis for a finding either way. For a target with little logging, the report states the narrower basis plainly and gives a clean result its exact weight. The report states the evidence, its depth of coverage and the monitoring after close that would extend it.

What should the target preserve before the assessment?

Ask for log exports from the firewall, identity provider, endpoint platform and cloud tenants to be preserved at their current retention with rolling deletion paused, for asset inventories and architecture diagrams as they exist, for prior penetration test and audit reports with remediation records, for incident history including insurance claims, and for a list of all privileged and service accounts. Ask that cleanup, reimaging and configuration changes in the environment be scheduled with notice to the acquirer and held until the assessment is complete.

How do your findings get used in the purchase agreement?

Each finding is reported with its technical basis, its remediation cost and its risk to integration and compliance, in plain terms. Deal counsel typically turns those into specific representations about incident history and control status, indemnities or escrows sized to the remediation estimate, closing conditions for critical fixes and post close covenants for monitoring. Our role is the evidence and the technical judgment. The legal structure belongs to the lawyers, and we write the report so the two connect cleanly.

Web Addresses for the Sources Cited

1. four business days: https://www.sec.gov/newsroom/press-releases/2023-139
2. SHIELD Act: https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act
3. 45 CFR 164.404: https://www.law.cornell.edu/cfr/text/45/164.404
4. NIST Cybersecurity Framework 2.0: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final
5. NIST SP 1305: https://csrc.nist.gov/pubs/sp/1305/final
6. cybersecurity risk management and incident disclosure rule: https://www.sec.gov/rules-regulations/2023/07/s7-09-22

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.