What to Check Before You Buy a Web-Based Business

A pre-close technical risk inventory for buyers of web-based businesses.

Danielle Voorhees, Veritech Diligence

Why this document exists

Most technical due diligence guidance available online is written for buyers of mid-market SaaS companies with dedicated engineering teams, defined stacks, and structured data rooms. That guidance does not translate cleanly to the businesses that trade on Acquire.com, Flippa, or through quiet broker deals. A web-based business at this deal size does not have a Chief Technology Officer to interview. It has a founder or a lean team who built the systems while running the company, who documented very little of what they did, and who will be gone within thirty to ninety days of close.

The risk in that situation is not concentrated in any single system. It is distributed across nine layers of the business, and those layers are held together by working knowledge that leaves the building at handoff. The buyer inherits the layers. The buyer does not inherit the knowledge.

This document walks through each of those layers, explains what to check before you sign, and points to the specific red flags that signal a target is more fragile than the seller has represented. Use it as a scoping document during your evaluation window, share it with your advisors, and mark any layer where the answers feel evasive or the systems feel undocumented. Those layers are where valuation adjustments live.

A note on scope: this is a checklist for what to look at, not a substitute for hands-on inspection. Several layers below require access to code, servers, or admin panels that a non-technical buyer cannot practically evaluate without help. Where that is true, this document says so directly.

Layer 1: Analytics and Data Integrity

The numbers in the deal deck all come from somewhere, usually a Google Analytics 4 property, a Meta Pixel, or a set of dashboards built on top of them. Before you accept any traffic, conversion, or revenue-attribution figure at face value, you need to verify that the underlying tracking is configured correctly and reports the events it claims to report.

Web-based businesses at this deal size have an analytics stack that was almost always set up quickly and modified over time without documentation. That produces three predictable problems. Events double-fire because the same conversion is tracked by both a page view and a purchase event. Server-side and client-side tracking run in parallel without proper deduplication, inflating reported conversions by fifteen to forty percent. Historical data breaks silently at some point in the past when the property was migrated or a tag was updated, and nobody noticed because the dashboards still populate.

Red flags to look for in the evaluation window

The GA4 property creation date does not match the age of the business as represented. A three-year-old business with a property created eight months ago has either lost its historical data or is showing you numbers that do not go back as far as claimed. Check the property creation date in the admin panel before you look at any other number.

Conversion rates that are suspiciously consistent month over month, especially in the range of two to four percent. Real ecommerce and content businesses show meaningful seasonal and campaign-driven variance. A flat conversion rate suggests either aggressive filtering, inflated denominators, or manual reporting rather than pulled data.

Traffic that comes overwhelmingly from a single source, particularly organic search or a single referrer domain, without a documented explanation. Concentration is not automatically a problem, but it needs a story.

Meta Pixel and Google Ads conversion counts that exceed GA4 purchase counts by more than a small margin. This is the classic sign of client-side and server-side events firing without deduplication.

Reported revenue in the deck that does not reconcile with Stripe, Shopify, or the payment processor of record. Ask for both figures for the same period and check them yourself.

What this layer requires from a professional review:

An audit of the tag manager container to confirm event architecture, an inspection of the GA4 event stream for duplicates and misconfigurations, and a check of Consent Mode configuration where the business operates in jurisdictions with cookie regulation. Remediation of a broken analytics stack typically takes hours of skilled work, but the more consequential outcome of the audit is the answer to whether the numbers in the deck are real. A finding here changes the offer.

Layer 2: Platform and Codebase Architecture

The codebase and content management platform are the second layer where inherited risk is real. These businesses are rarely running the clean, modern stacks that technical due diligence guidance assumes. They are running WordPress with a page builder layered on top of a decade of plugin decisions, or Drupal with a series of custom modules nobody has documented, or a half-completed headless migration where the old and new systems both still serve traffic.

The differences from an enterprise stack are structural. There is no separation between development, staging, and production. There is no version control history, or the history exists but the current live site does not match the repository. Plugins and modules were installed to solve specific problems and never removed when the problem went away, leaving thirty or forty active pieces of code the current owner cannot fully account for. Custom code was written directly into theme files rather than into a child theme or a plugin, meaning any theme update overwrites it.

Red flags to look for

The seller cannot name the current versions of the CMS, the theme, and the top five plugins by usage. This is a fair question to ask in a call, and an evasive answer tells you the seller has not touched the technical side of the business in some time.

The site runs on a page builder, especially Elementor Pro, Divi, WPBakery, or Breakdance, without a documented explanation of which builder controls which pages. Multiple page builders on the same site is a specific warning sign of accumulated debt.

There is no staging environment, or the staging environment does not match production. Ask directly whether changes are tested before they go live. If the answer is no, or vague, plan for staging setup as a day-one cost.

The most recent core, theme, and plugin update dates are more than sixty days old. Small updates skipped for months turn into large updates that break things, and unpatched plugins are the most common vector for site compromise.

There is no documentation of custom code, custom post types, or custom functionality. The seller can show you the site works, but cannot show you how it works.

Paid plugins, themes, or third-party licenses are tied to the seller's personal account rather than a business account. Some licenses transfer cleanly with a change of ownership; others require repurchase, and a few have seat limits that can lock the buyer out entirely until a new license is issued.

Critical licenses are near renewal or already lapsed, and losing them would break core site functionality. A lapsed page builder or plugin license does not always break the site immediately, but it usually blocks updates and support, which becomes a problem the first time something needs fixing.

Custom code was built by a contractor or agency with no signed IP assignment or work-for-hire agreement on file. Without that paperwork, the business may not actually own the code it is selling, and the buyer inherits that ambiguity along with the site.

The live site does not match what is in the repository, or no repository exists at all. If the buyer cannot build and deploy the current site from source control alone, they are relying entirely on the production server never failing.

There is no rollback procedure for a failed deployment, and updates are applied ad hoc without a change log. A site with no record of what changed and when is a site where the next update is a guess, not a plan.

Critical user journeys, such as checkout or lead capture, are not retested after changes go live. Regressions in the paths that generate revenue are the most expensive kind, and they are the first thing to break silently after an untested update.

This layer generally cannot be evaluated by a non-technical buyer.

A professional review covers a plugin and module inventory with versions and last-update dates, an assessment of custom code and where it lives in the codebase, a review of the theme structure for child theme compliance and update safety, a check of the repository against the live site, and an evaluation of the update pipeline. Remediation of accumulated codebase debt ranges widely, from a few days for a well-maintained site with modest cleanup needs to several weeks for a site where custom code must be extracted from theme files and rebuilt in a maintainable structure. The variance itself is the finding: a buyer should not commit to a purchase price without knowing which end of that range they are inheriting.

Layer 3: Ecommerce and Payment Infrastructure

For any business that processes payments, revenue-recognition risk lives in this layer. Subscription billing, one-time checkout, refund handling, chargeback processing, and PCI compliance all sit here, and a misconfiguration in any of them creates either revenue leakage or legal exposure.

Web-based ecommerce businesses generally use WooCommerce, Shopify, or a lightweight custom checkout on top of Stripe. WooCommerce is the most common and the most fragile, because it runs on top of WordPress and inherits every problem the platform layer has. WooCommerce Subscriptions, in particular, is a common source of quiet failure. Subscriptions that were set up years ago on old versions of the plugin may not renew correctly. Failed payments may not trigger dunning emails. Cancellations may not process refunds. The seller often does not know any of this is happening, because the dashboard shows healthy total subscriber counts.

Red flags

The reported monthly recurring revenue does not match the actual sum of active subscriptions in the payment processor. This is a direct arithmetic check and the discrepancy is often material.

Failed payment volume is not reported in the deal deck at all. Every subscription business has a failed payment rate. If the seller cannot tell you what theirs is, they are not monitoring their revenue.

There is no documented refund policy or refund process. These businesses often handle refunds manually, and the manual process leaves with the departing owner and creates a service gap on day one.

The checkout is customized in ways the seller cannot fully explain, particularly custom checkout fields, custom shipping calculations, or custom tax handling. Custom code in the checkout path is a common source of dropped orders that the seller does not know about because the customer simply gave up and left.

PCI compliance status is unknown or has not been reviewed in the past twelve months. A buyer taking over a business that is non-compliant inherits both the compliance obligation and the liability for any prior period.

Payment gateway account is in the seller's name and cannot be transferred cleanly. This is not exactly a technical risk, but it appears in the same review and delays closing.

What a professional review covers

A reconciliation of reported subscription revenue against the payment processor, an inventory of custom checkout code and where it lives, a review of failed payment and chargeback rates, a check of PCI configuration and compliance status, and a mapping of the payment gateway ownership and transfer requirements. Remediation of a broken subscription pipeline is often the highest-value finding in an ecommerce diligence engagement, because a two percent recovery of previously lost renewals compounds over the ownership period.

Layer 4: Infrastructure, Deployment, and Performance

Hosting and server configuration determine what the business can survive after close. Under-provisioned hosting produces performance problems that look cosmetic but are actually structural. A site that "feels slow" often has a root cause buried in database query

design or caching misconfiguration, not something a generic performance scan will surface, and the root cause is what determines whether the fix is straightforward or expensive.

Businesses at this deal size are usually hosted on shared hosting, on a low-tier managed host, or on a single virtual private server that was configured once and never revisited. The caching layer is often doing more work than the underlying infrastructure, meaning the site appears fast because Redis or a CDN is masking a slow database. When a new owner logs in and starts making changes, the cache gets invalidated and the real performance profile shows.

Red flags

Core Web Vitals scores in the poor range for either LCP or INP on mobile. This is a check you can run yourself using Google PageSpeed Insights on the target's homepage and top three revenue-driving pages. Consistently poor mobile scores are both a search ranking problem and a signal of infrastructure debt.

The seller cannot name the host or the hosting plan. This happens more often than you would expect. It usually means hosting is auto-billed to a personal credit card and the technical setup has not been touched in years.

There is no CDN, or there is a CDN whose configuration nobody has audited. A misconfigured CDN can serve stale content to some visitors and fresh content to others, which is difficult to diagnose after close.

The site has been migrated between hosts within the past twelve months. Recent migrations often leave behind broken configurations, orphaned files, and DNS artifacts that surface weeks later.

SSL certificates are near expiration, or are configured manually rather than through automatic renewal. A certificate that expires the week after close is a common and preventable outage.

There is no monitoring or alerting configured. The seller finds out the site is down when a customer emails them. A buyer inherits that same detection lag.

There is no defined recovery time or recovery point objective, so nobody knows how much data or downtime an outage would actually cost. Without those two numbers, “we have backups” is not a real answer to “how bad would it be.”

Monitoring, where it exists, does not cover checkout, forms, or other revenue-critical paths, only the homepage or basic server uptime. A site can show as “up” while its checkout is silently broken for hours.

Alerts are not tuned to anything meaningful, or they go to an inbox nobody actively monitors. An alert nobody reads is functionally the same as no alert at all.

Monitoring and alerting tools are configured under the seller’s personal account and will stop working the moment that account is closed. This is easy to miss during a transition, since everything looks fine right up until it silently doesn’t.

What a professional review covers

Server log analysis, database query profiling, caching layer audit, CDN configuration review, SSL and DNS check, and a Core Web Vitals root-cause analysis rather than a surface scan.** Remediation ranges from a few hours of caching configuration to a full hosting migration, depending on findings.

Layer 5: Security

Security risk in a web-based business acquisition at this deal size falls into two categories: known vulnerabilities that have not been patched, and unknown compromises that have already occurred. The buyer inherits both.

The most common security failure at this deal size is not a sophisticated attack. It is an outdated plugin with a known vulnerability, exploited by an automated scanner, that installed backdoor code the current owner never noticed. The site continues to function normally. Traffic looks normal. The compromise surfaces months later when the site starts serving spam pages to search engines, or when the hosting provider quarantines the account.

Red flags

Plugins, themes, or CMS core are running versions with published Common Vulnerabilities and Exposures records. This can be checked against the WordPress vulnerability database or equivalent for Drupal and other platforms, though it requires knowing which versions are installed.

There is no record of past security incidents, and the seller cannot describe how they would know if the site were compromised. The absence of a monitoring history is not proof of the absence of compromise.

Admin accounts are shared or use weak passwords. This is a direct question to ask: how many admin accounts exist, who owns them, and are any of them shared credentials.

There is no web application firewall, or the firewall is a free tier that has not been configured beyond default settings.

The site accepts user uploads and does not restrict file types or scan uploads. This is a specific vector that produces most of the compromises this document is describing.

Backup strategy is undocumented or non-functional. Ask when the last successful restore from backup was tested. If the answer is never, the backups are not real backups.

Former employees or contractors still have active access to admin panels, hosting, or code repositories. Access that was never revoked is access nobody is thinking about until it's misused.

There is no least-privilege model; every user with any access has full admin rights. A support contractor with full admin access is a bigger blast radius than the task ever required.

Password recovery for critical accounts depends on the seller's personal email or phone number. If that recovery path breaks the day after close, the buyer may be locked out of their own systems with no clean way back in.

There is no documented emergency access procedure if the primary admin becomes unreachable. Plan for the version of this problem that happens on a weekend.

Assessment of this layer requires access to server logs, admin accounts, and often the file system.

A professional review covers a vulnerability scan against known CVE databases, a review of admin access and authentication, a check for indicators of compromise in server logs and file system, a review of backup strategy with a test restore, and a firewall configuration audit. Remediation of an active compromise is more expensive than remediation of an unpatched vulnerability, which is why the timing of this check matters. A finding here can also expose the buyer to disclosure obligations depending on jurisdiction and data handling, which is worth flagging to legal counsel immediately.

Layer 6: SEO and Organic Channel Value

Organic search traffic is often a meaningful part of the valuation story for a content or ecommerce business, and it is a category where the numbers can look stable in a screenshot while declining underneath. Technical SEO configuration is also fragile in a specific way: a new owner making apparently minor changes to the site can inadvertently break the configuration that produces the organic traffic they just bought.

Red flags

Organic traffic has declined by more than fifteen percent over the past twelve months without a documented cause. Google Analytics and Google Search Console will both show this. Ask for direct access to both, or ask for screenshots covering at least the past eighteen months.

The site has never migrated to GA4 properly, or the GA4 property is missing organic traffic data for a meaningful period. This is a common pattern from the Universal Analytics sunset in mid-2023.

Ranking positions are concentrated in a small number of keywords driving a majority of the traffic. Ask for the top ten pages by organic traffic and the top ten keywords driving that traffic. If the concentration is high, ranking volatility on any one of those keywords becomes a significant revenue risk.

The site uses aggressive redirects, canonical URLs pointing to unexpected destinations, or hreflang configurations that do not match the current content. Any of these can indicate a prior SEO strategy that a new owner will inadvertently unwind.

Backlink profile shows a high proportion of low-quality or paid links. This is a check that requires a tool like Ahrefs, SEMrush, or Conductor, but it is worth doing before close because a manual action or algorithmic penalty inherited from a prior link-building strategy is not recoverable through remediation.

There is no XML sitemap, or the sitemap does not match the site's actual URL structure. This is a small technical detail that signals broader technical SEO neglect.

What a professional review covers

An audit of technical SEO configuration including schema markup, canonical URLs, sitemaps, and redirects, a review of Google Search Console for manual actions or crawl issues, a backlink profile analysis, a ranking concentration review, and a check of how organic traffic maps to revenue by page. Remediation of technical SEO issues ranges from days to weeks depending on findings. Recovery from a penalty or a manual action ranges from months to never.

Layer 7: Accessibility and Compliance

Accessibility non-compliance is a legal exposure category that most technical due diligence providers do not check, and it is one of the most common surprise findings after close. Accessibility lawsuits against ecommerce and content businesses at this deal size have been rising steadily. Settlement costs typically fall between five and twenty thousand dollars per complaint, and a buyer inherits the exposure the moment they take ownership.

Red flags

The site has no accessibility statement, or the statement is generic boilerplate. Real accessibility statements describe the standards the site aims to meet and the mechanism for reporting problems.

Images throughout the site lack alt text, or alt text is generic or auto-generated. This is a check a buyer can perform directly by inspecting the page source or using a browser accessibility extension.

Forms lack labels, or labels are not associated with their inputs. This is a specific failure that screen readers cannot work around.

Color contrast on primary call-to-action elements and body text falls below WCAG 2.1 AA standards. This is checkable with any browser-based contrast tool.

The site uses a third-party accessibility overlay widget as its compliance strategy. Accessibility overlays have been the subject of specific and successful litigation, and their presence is a signal rather than a mitigation.

There is no record of prior accessibility audits or user testing with assistive technology users.

Beyond accessibility, this layer also covers cookie consent compliance for jurisdictions with GDPR, CCPA, or similar frameworks, and disclosure and terms-of-service pages that reflect the site's actual data handling. A quick review of these documents against the site's actual behavior often finds gaps.

Nobody can say where customer and user data is actually stored, or for how long it's retained in databases, logs, and backups. A business that can't answer this can't credibly claim compliance with any data protection framework, regardless of what its privacy policy says.

Deleted records are only soft-deleted and remain fully recoverable, which may directly contradict the site's own privacy policy. This is a common and serious gap between stated policy and actual system behavior.

Backups contain personal or sensitive data with no separate retention or access policy from production. A backup is not exempt from the same data protection obligations as the live system.

Staging and production environments share live customer data, creating a second, less-secured copy of sensitive information. Staging environments are rarely hardened to the same standard as production, which makes this a real and common leak point.

A professional review of this layer

Produces a WCAG 2.1 compliance report, a cookie consent configuration audit, and an inventory of privacy policy and terms of service gaps.** Remediation of accessibility issues ranges from a day of focused work for a simple content site to several weeks for a complex ecommerce site with custom interactive elements. The remediation cost is almost always less than the cost of a single lawsuit.

Layer 8: Automation, Integration, and Operational Fragility

This layer is where web-based business acquisitions most commonly fail after close, and it is the layer that formal diligence checklists most commonly overlook. A modern business at this deal size is held together by a web of automations: a Zapier workflow that moves customers from Stripe to the email platform, an n8n instance that syncs inventory between the website and a third-party fulfillment provider, a set of API keys embedded in code that connect the site to a CRM, an ERP, or a payment gateway.

The seller knows how these automations work because they built them. The documentation, if it exists, is a mix of screenshots, half-finished Notion pages, and undocumented API keys in a password manager. When the seller leaves, the automations continue running until something breaks, and when something breaks, the buyer has no map for how to fix it.

Red flags

The seller cannot produce a written inventory of every third-party service the business depends on, with account ownership, billing responsibility, and login credentials. This inventory is a basic diligence artifact and its absence is a diligence finding on its own.

There is a Zapier, Make, or n8n account whose task history the seller cannot fully explain. Ask to see the active workflows and ask what each one does. Vague answers signal accumulated automations that nobody has audited.

Email marketing automation flows are extensive and undocumented. A business with fifty active email automations and no map of what triggers what is a business whose customer communications will break the first time a new owner touches the platform.

API keys and credentials for third-party services are stored in personal password managers or personal email accounts. Transfer of these credentials is not automatic and often not clean.

Integrations run between services that are billed to personal accounts of the seller or of a former employee. This is common and easy to miss until a bill fails and a service disconnects.

There is no runbook for common operational tasks. Ask the seller to describe what happens when a customer requests a refund, when a subscription payment fails, when an order needs to be shipped, or when the site goes down. Vague answers here predict operational failures after close.

The domain registrar account is in the seller's personal name, and no transfer process has been discussed. A technical stack is not truly acquired if the buyer doesn't control the domain it runs on.

DNS is managed through an account the seller controls, with no documented transfer plan or backup access. Losing DNS access, even briefly, can take email and the entire site offline at once.

Analytics, tag manager, ad platform, or payment gateway accounts are personal rather than business accounts, and transferability hasn't been confirmed. Each of these is a separate point where the buyer can end up locked out on day one.

There is no backup admin contact or two-factor recovery method for any critical account. A single lost phone or forgotten password on the seller's end can lock the buyer out of systems they now legally own.

Automations have no fallback behavior when a connected service goes down, and failures are not monitored, they simply fail silently. The business runs fine until the moment it doesn't, and nobody notices until a customer complains.

A professional review of this layer

Produces an integration map showing every third-party service, every automation workflow, every API connection, and every credential ownership relationship. This is often the single most useful deliverable a buyer receives from a technical diligence engagement, because it is the map the new owner needs on day one and the seller cannot produce.

Layer 9: Concentrated Knowledge Risk

The eight technical layers above are individually assessable. Each of them can be checked, documented, and remediated. The ninth layer is different, and it is the layer that changes how a buyer should think about the previous eight.

Web-based businesses at this deal size concentrate operational knowledge in one or a small number of people. Whether the business is run by a solo founder or by a team of three, the knowledge of how the systems work together, why they were built the way they were built, and what breaks when a particular change is made, lives in the head of the person or people who built it. Documentation, when it exists, describes what the systems are, not why the systems are the way they are.

That knowledge does not transfer at close. The seller signs a transition support agreement, typically covering thirty to ninety days, and during that window the buyer has access to the seller’s answers. After that window, the buyer has the systems and does not have the reasoning. Every technical decision the buyer makes after that point is made without the context that would have prevented the decision from breaking something the buyer did not know was connected.

This is why a diligence process that assesses the eight layers in isolation is insufficient. The findings from those eight layers describe the current state of the systems. They do not describe the risk of operating the systems without the knowledge that built them. Two businesses can have identical technical debt profiles and represent completely different risk exposures based on how much of the operating knowledge is documented and how much is concentrated in the seller.

A diligence engagement that addresses this layer produces two things a checklist-based review does not. First, an assessment of documentation quality across all eight technical layers, distinguishing between what is written down and what only exists in the seller's working memory. Second, a prioritized list of the knowledge that most urgently needs to be extracted during the transition window, before the seller's context becomes unreachable.

Red flags that indicate high concentrated knowledge risk

The seller can answer any technical question you ask, immediately and fluently, without referring to documentation. This is a signal that the documentation does not exist.

The transition support agreement is short, informal, or vaguely defined. A seller who is not committing to a substantial and structured handoff is a seller who does not understand how much of the business lives only in their head.

There is a "person who handles the tech" who is not part of the sale, whether that is a contractor, a former employee, or a friend. Business continuity that depends on someone outside the transaction is business continuity that does not survive the transaction.

Prior owner transitions, if any, are described as difficult or as producing outages. Businesses that have transitioned poorly before will transition poorly again unless the underlying documentation gap has been addressed.

The seller's own documentation of the business, whether an internal wiki or a set of runbooks, is thin, out of date, or nonexistent. Ask to see it. The gap between what the seller shows you and what you would need to operate the business is the concentrated knowledge risk quantified.

A related risk sits on top of all nine layers above: whether anyone has ever mapped which systems are genuinely load-bearing and which are redundant. Most sellers have never had to find out, because nothing has forced the question.

Nobody can say what happens to checkout, email, or reporting if hosting, DNS, or a core integration goes down for an hour. If the answer is a shrug, that's the finding.

The business has never lost a single point of failure and recovered gracefully, so nobody actually knows where the fragile seams are. Untested resilience is not the same as real resilience.

Mapping every dependency and its blast radius across all nine layers is exactly what a full technical review produces. It is not something a buyer can reliably build alone inside a single evaluation window, and a partial map is often worse than no map, since it creates false confidence in exactly the places it missed.

Summary Checklist

A working artifact for your evaluation window. Print it, mark it up, share it with your advisors. For each item below, mark whether it's not a concern, a minor concern worth monitoring, or a material concern that affects the offer.

How to use this checklist

Work through the layers in order, flag anything that reads as evasive or undocumented, and score each layer by finding density. Yellows translate to a price adjustment or an escrow holdback; reds in security, accessibility, or concentrated knowledge usually mean renegotiation or walking away.

Several layers need access and expertise beyond what a non-technical buyer can bring alone. There, this checklist is a scoping document, shared vocabulary for you, your advisors, and whoever runs the professional review.

This document is licensed for free distribution. Share it with your advisors, your co-investors, and your broker. It exists to be used.

Layer 1: Analytics and Data Integrity

ITEM	GREEN	YELLOW	RED
GA4 property creation date doesn't match business age as represented	☐	☐	☐
Conversion rates suspiciously flat month over month	☐	☐	☐
Traffic concentrated in a single source without a documented explanation	☐	☐	☐
Meta Pixel or Google Ads conversion counts exceed GA4 by more than a small margin	☐	☐	☐

ITEM	GREEN	YELLOW	RED
Reported revenue in the deck doesn't reconcile with the payment processor	☐	☐	☐

Layer 2: Platform and Codebase Architecture

ITEM	GREEN	YELLOW	RED
Seller can't name current versions of CMS, theme, and top plugins	☐	☐	☐
Site uses multiple page builders without a documented explanation	☐	☐	☐
No staging environment, or staging doesn't match production	☐	☐	☐
Core, theme, and plugin update dates are more than 60 days old	☐	☐	☐
No documentation of custom code, custom post types, or custom functionality	☐	☐	☐
Paid plugins, themes, or licenses tied to seller's personal account	☐	☐	☐
Critical licenses near renewal or lapsed	☐	☐	☐
Custom code built by a contractor with no signed IP assignment	☐	☐	☐
Live site doesn't match repository, or no repository exists	☐	☐	☐
No rollback procedure or change log for deployments	☐	☐	☐
Critical user journeys not retested after changes go live	☐	☐	☐

Layer 3: Ecommerce and Payment Infrastructure

ITEM	GREEN	YELLOW	RED
Reported MRR doesn't match sum of active subscriptions in payment processor	☐	☐	☐
Failed payment volume not reported in the deal deck	☐	☐	☐
No documented refund policy or refund process	☐	☐	☐
Custom checkout code the seller can't fully explain	☐	☐	☐
PCI compliance status unknown or not reviewed in past 12 months	☐	☐	☐
Payment gateway account in seller's name and not cleanly transferable	☐	☐	☐

Layer 4: Infrastructure, Deployment, and Performance

ITEM	GREEN	YELLOW	RED
Core Web Vitals in poor range for LCP or INP on mobile	☐	☐	☐
Seller can't name the host or hosting plan	☐	☐	☐
No CDN, or CDN configuration nobody has audited	☐	☐	☐
Site migrated between hosts within the past 12 months	☐	☐	☐
SSL certificates near expiration or configured manually	☐	☐	☐
No monitoring or alerting configured	☐	☐	☐
No defined recovery time or recovery point objective	☐	☐	☐

ITEM	GREEN	YELLOW	RED
Monitoring doesn’t cover checkout, forms, or revenue-critical paths	☐	☐	☐
Alerts untuned or sent to an unmonitored inbox	☐	☐	☐
Monitoring tools tied to seller’s personal account	☐	☐	☐

Layer 5: Security

ITEM	GREEN	YELLOW	RED
Plugins, themes, or CMS core running versions with published CVEs	☐	☐	☐
No record of past security incidents and no way to detect one	☐	☐	☐
Admin accounts shared or using weak passwords	☐	☐	☐
No web application firewall, or default-configured free tier only	☐	☐	☐
Site accepts user uploads without file-type restriction or scanning	☐	☐	☐
Backup strategy undocumented or last successful restore never tested	☐	☐	☐
Former employees or contractors retain active access	☐	☐	☐
No least-privilege access model in place	☐	☐	☐
Password recovery depends on seller’s personal email or phone	☐	☐	☐
No documented emergency access procedure	☐	☐	☐

Layer 6: SEO and Organic Channel Value

ITEM	GREEN	YELLOW	RED
Organic traffic declined more than 15% in past 12 months without cause	☐	☐	☐
GA4 migration incomplete or missing organic traffic data	☐	☐	☐
Ranking positions concentrated in a small number of keywords	☐	☐	☐
Aggressive redirects, unexpected canonicals, or mismatched hreflang	☐	☐	☐
Backlink profile shows high proportion of low-quality or paid links	☐	☐	☐
No XML sitemap, or sitemap doesn't match site URL structure	☐	☐	☐

Layer 7: Accessibility and Compliance

ITEM	GREEN	YELLOW	RED
No accessibility statement, or statement is generic boilerplate	☐	☐	☐
Images throughout site lack alt text or use auto-generated text	☐	☐	☐
Forms lack labels, or labels not associated with inputs	☐	☐	☐
Color contrast on primary elements below WCAG 2.1 AA	☐	☐	☐
Site uses a third-party accessibility overlay widget	☐	☐	☐
No record of prior accessibility audits or assistive-technology testing	☐	☐	☐
Nobody can say where customer data is stored or how long it's retained	☐	☐	☐

ITEM	GREEN	YELLOW	RED
Deleted records are only soft-deleted, contradicting stated policy	☐	☐	☐
Backups contain sensitive data with no separate retention policy	☐	☐	☐
Staging and production share live customer data	☐	☐	☐

Layer 8: Automation, Integration, and Operational Fragility

ITEM	GREEN	YELLOW	RED
Seller can’t produce written inventory of every third-party service	☐	☐	☐
Zapier, Make, or n8n workflows the seller can’t fully explain	☐	☐	☐
Extensive email marketing automation flows without documentation	☐	☐	☐
API keys stored in personal password managers or personal email	☐	☐	☐
Integrations billed to personal accounts of seller or former employees	☐	☐	☐
No runbook for common operational tasks	☐	☐	☐
Domain registrar account in seller’s personal name, no transfer plan	☐	☐	☐
DNS managed through seller’s account with no documented transfer plan	☐	☐	☐
Analytics, ad, or payment gateway accounts are personal, not business	☐	☐	☐
No backup admin contact or 2FA recovery for critical accounts	☐	☐	☐
Automations have no fallback behavior and failures aren’t monitored	☐	☐	☐

Layer 9: Concentrated Knowledge Risk

ITEM	GREEN	YELLOW	RED
Seller answers any technical question fluently without referring to docs	☐	☐	☐
Transition support agreement is short, informal, or vaguely defined	☐	☐	☐
A “person who handles the tech” is not part of the sale	☐	☐	☐
Prior owner transitions described as difficult or producing outages	☐	☐	☐
Internal wiki, runbooks, or documentation thin, stale, or nonexistent	☐	☐	☐
Nobody can say what happens if hosting, DNS, or a core integration goes down	☐	☐	☐
Business has never tested recovery from a single point of failure	☐	☐	☐

Scoring guidance. A single yellow finding is typically a remediation estimate and a modest offer adjustment. A pattern of yellows across multiple layers signals broader fragility, and calls for either a price reduction, a longer transition commitment, or a portion of the purchase price held in escrow. Reds in Security, Accessibility, or Concentrated Knowledge warrant substantive renegotiation or a decision to walk.

About this document

This inventory reflects fifteen years of work across the specific stack that web-based businesses at this deal size actually run: WordPress and WooCommerce, Drupal, headless and decoupled CMS builds, custom checkout and subscription systems, GA4 and Google Tag Manager, server-side tracking, hosting and caching layers, and the automation platforms that hold everything together. The author is a published GA4 implementation

author and has led technical work across analytics, ecommerce, security, and platform migration for over fifteen years, including for enterprise clients and independent businesses acquired through the same channels described here.

If you would like a full technical review run against a specific target during your evaluation window, Veritech Diligence offers scoped engagements covering all nine layers above, with turnaround times matched to search fund, independent sponsor, and holding company timelines. Contact information at veritechdiligence.com.

From **What to Check Before You Buy a Web-Based Business** *by Danielle Voorhees, Veritech Diligence. Full inventory at veritechdiligence.com.*