

The Pre-Close Checklist

A companion to the full risk inventory, What to Check Before You Buy a Web-Based Business, at veritechdiligence.com.

Danielle Voorhees, Veritech Diligence

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.

Some of the checklist items are things you or your broker should ask the seller directly; evasive or vague answers are a potential finding. Others require hands-on access to code, logs, and admin panels that only a technical review can properly assess. A Veritech Diligence engagement covers the second category: systems, configurations, and data, but not seller interviews.

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.*