

50 Technology Questions to Ask Before Buying a Dealership

Use this checklist during early diligence to identify unclear ownership, unsupported systems, security gaps, contract exposure, and Day One dependencies.

How to use it

Ask each question, identify the evidence needed, assign an owner, and record unresolved items in the acquisition workbook. Do not place passwords or customer information on this checklist.

Ownership and control

[] 1	Who legally owns and controls every dealership domain name?	Owner _____ Evidence _____
[] 2	Are registrar, DNS, and certificate credentials verified and protected by MFA?	Owner _____ Evidence _____
[] 3	Who controls the Microsoft 365 or Google tenant and global administrator accounts?	Owner _____ Evidence _____
[] 4	Which administrative accounts are held by the seller, an employee, or an MSP?	Owner _____ Evidence _____
[] 5	Are service, shared, emergency, and vendor accounts identified and assigned to owners?	Owner _____ Evidence _____
[] 6	Is there a complete employee roster mapped to locations, departments, managers, systems, and devices?	Owner _____ Evidence _____
[] 7	Are terminated and dormant accounts disabled across every critical system?	Owner _____ Evidence _____
[] 8	Will any identity provider, SSO configuration, tenant, or email domain change at close?	Owner _____ Evidence _____

Connectivity and infrastructure

[] 9	Which Internet circuits serve each building, annex, warehouse, and remote lot?	Owner _____ Evidence _____
[] 10	What are the carrier, bandwidth, circuit ID, public IP, contract term, and service address for each circuit?	Owner _____ Evidence _____
[] 11	Will any circuit or public IP change when ownership transfers?	Owner _____ Evidence _____
[] 12	Is tested backup Internet available at each operationally critical building?	Owner _____ Evidence _____
[] 13	Who owns the firewalls, switches, access points, wireless links, racks, and cabling?	Owner _____ Evidence _____
[] 14	Are current network diagrams, VLANs, IP ranges, VPNs, and routing dependencies documented?	Owner _____ Evidence _____
[] 15	Are network administrative credentials available and tested?	Owner _____ Evidence _____
[] 16	Are unsupported network devices or expired support contracts identified?	Owner _____ Evidence _____

Applications and data

[] 17	Which DMS products, modules, stores, company numbers, and environments are in use?	Owner _____ Evidence _____
[] 18	Which CRM, desking, F&I, digital retail, inventory, service, parts, payroll, and accounting systems are active?	Owner _____ Evidence _____
[] 19	Which integrations, APIs, file feeds, SSO connections, scheduled jobs, printers, and public IP allow lists are required?	Owner _____ Evidence _____
[] 20	Who owns the data, and which exports must be completed before close?	Owner _____ Evidence _____
[] 21	Are application licenses, administrators, users, roles, and store mappings documented?	Owner _____ Evidence _____
[] 22	Which applications or services terminate at change of ownership?	Owner _____ Evidence _____
[] 23	Are file shares, cloud drives, local files, and historical reports included in the transition plan?	Owner _____ Evidence _____
[] 24	Are data retention, preservation, transfer, return, and secure deletion obligations documented?	Owner _____ Evidence _____

Cybersecurity and continuity

[] 25	Is there a written information security program and a named qualified individual?	Owner _____ Evidence _____
[] 26	Is a current written risk assessment available?	Owner _____ Evidence _____
[] 27	Which endpoint protection, vulnerability management, SIEM, SOC, monitoring, and email-security services are active?	Owner _____ Evidence _____
[] 28	Will any security service stop or change at close?	Owner _____ Evidence _____
[] 29	Are open vulnerabilities, security exceptions, prior incidents, and insurance claims disclosed to the appropriate reviewers?	Owner _____ Evidence _____
[] 30	Are backups encrypted, isolated, current, and tested through representative restores?	Owner _____ Evidence _____
[] 31	Are incident response, business continuity, and outage procedures current?	Owner _____ Evidence _____
[] 32	Are privileged accounts, local administrator rights, remote access, and MFA reviewed?	Owner _____ Evidence _____

Vendors and contracts

[] 33	Is there a complete technology vendor and contract register supported by invoices and general-ledger review?	Owner _____ Evidence _____
[] 34	Which agreements are assumed, excluded, assignable, or subject to change-of-control consent?	Owner _____ Evidence _____
[] 35	What are the monthly and annual costs, renewal dates, notice periods, auto-renewal terms, and early termination fees?	Owner _____ Evidence _____
[] 36	Which products overlap or duplicate another service?	Owner _____ Evidence _____
[] 37	Which equipment is leased, seller-owned, MSP-owned, OEM-managed, or owned by the dealership?	Owner _____ Evidence _____
[] 38	Which service providers can access customer information, and what oversight evidence is available?	Owner _____ Evidence _____
[] 39	Who are the primary and escalation contacts for every critical vendor?	Owner _____ Evidence _____

Day One operations

☐ 40	Are merchant accounts, payment gateways, terminals, settlement accounts, and integrations ready for the buyer?	Owner _____ Evidence _____
☐ 41	Are telephone numbers, porting authority, call flows, queues, voicemail, fax, paging, and E911 documented and tested?	Owner _____ Evidence _____
☐ 42	Are OEM portals, dealer codes, diagnostic equipment, certificates, VPNS, and change-of-ownership steps ready?	Owner _____ Evidence _____
☐ 43	Are end-to-end tests prepared for sales, F&I, accounting, service, parts, payroll, payments, phones, and email?	Owner _____ Evidence _____
☐ 44	Can the buyer provide secure remote support and onsite coverage on Day One?	Owner _____ Evidence _____
☐ 45	Are temporary procedures ready for Internet, DMS, phone, email, payment, or security outages?	Owner _____ Evidence _____
☐ 46	Does every cutover task have an owner, dependency, execution window, status, and rollback procedure?	Owner _____ Evidence _____
☐ 47	Have unresolved Critical risks been resolved, covered by a tested contingency, or accepted in writing by an authorized executive?	Owner _____ Evidence _____
☐ 48	Is a Day 2 through Day 30 stabilization backlog ready?	Owner _____ Evidence _____
☐ 49	Is a buyer-controlled command channel ready with named decision-makers, vendor contacts, and escalation paths?	Owner _____ Evidence _____
☐ 50	Has the final go or no-go review confirmed backups, staffing, communications, test results, contingencies, and executive approval?	Owner _____ Evidence _____

Important This checklist supports operational due diligence. It does not provide legal advice, determine regulatory compliance, or replace a qualified security assessment.

techgurus.io