Culture & Conduct Diligence Checklist (Buyer-Side)

This buyer-oriented checklist is designed to surface latent cultural risks and conduct exposures that can materially affect value, integration, and reputational profile. It aligns diligence requests to observable metrics and identifies indicative red flags. Tailor scope to target size, sector, and regulatory posture.

Topic	What to Request	What to Review/Ask	Indicators/Red Flags
Leadership conduct and tone	Executive and senior leadership bios, performance evaluations, separation agreements for leaders in last 3 years	Assess leadership stability, performance culture, and documented misconduct issues	Undisclosed exits; repeated complaints; pay-to-muzzle NDAs; sudden, unexplained departures
Code of conduct and policy suite	Current Code of Conduct; Anti-Harassment/EEO; Whistleblowing; Conflicts of Interest; Anti-Bribery/Corruption; Gifts/Hospitality; Social Media; Remote Work; Supplier Code	Confirm version control, governance ownership, training cadence, translations, and acknowledgment rates	Outdated/no code; low acknowledgment completion; inconsistent global versions; no supplier code
Whistleblowing and investigations	Hotline/vendor contracts; case logs (anonymized), triage standards, time-to-close metrics; investigation protocols	Review case mix, root-cause analysis, remedial actions, board reporting, non-retaliation enforcement	Long closure times; discipline not commensurate; repeat allegations; retaliation claims; board blind spots
Harassment, discrimination, and retaliation	Complaint statistics; settlement/consent decrees; EEOC/agency filings; training completion data	Benchmark per capita rates; examine remediation quality and trendlines	Clusters in specific units; repeat offenders; systemic patterns; missing mandatory training
Culture health and engagement	Latest engagement survey instruments/results; pulse surveys; action plans; Glassdoor/Indeed trends; regretted attrition data	Correlate sentiment with attrition and productivity; evaluate response follow-through	No surveys; negative trend with no countermeasures; high regretted attrition in critical roles

DEI and pay equity	DEI strategy; representation by level; pay equity assessments; promotion/exit data; ERGs	Validate methodology, remediation actions, leadership sponsorship	No analyses; legal holds on pay data; persistent gaps without action
Incentives and sales conduct	Compensation plans for sales/BD; clawback policies; win-loss analysis; discounts/credit notes practices	Test for pressure to misreport; end-of-quarter “pull-ins”; return/chargeback patterns	Excessive SPIFFs; late adjustments; abnormal returns; “make the number at any cost” culture
Third-party conduct risk	Third-party risk framework; due diligence files; sanctions/ABAC screenings; audit results	Sample high-risk partners; examine approvals and monitoring	Incomplete due diligence; conflicts not mitigated; facilitation payment tolerance
Health, safety, and workplace behavior	Safety policies; incident/near-miss logs; OSHA/inspector findings; worker’s comp data; contractor controls	Look at severity rates, corrective action timeliness, contractor oversight	High TRIR/LTIR; repeat regulatory findings; material underreporting
Data ethics and engineering culture	Secure SDLC; code review standards; AI/ML ethics; privacy by design; model governance	Check adherence and exception handling; data minimization and consent	Production hotfix culture; no peer review; shadow datasets; unsafe model usage
Governance and oversight	Board/committee minutes on culture and conduct; KPI dashboards; policy approvals; training oversight	Map ownership, cadence, and escalation	No board visibility; stale dashboards; fragmented ownership
Integration readiness (if carve-out)	Local policy gaps; JV cultures; TUPE/works council/union posture; cultural integration plan	Identify conflicting norms, required consultations, and communication plan	Works council delays; conflicting union demands; culture clash without plan

Use this checklist to structure a document and data room request list, a management Q&A track, and a confirmatory close-out session. Where potential issues are identified, request underlying documents and conduct targeted interviews and sample testing.

Respectful Code Review Guidelines

Purpose and scope. These guidelines establish shared expectations for code reviews that are rigorous, respectful, and efficient. They apply to all contributors, whether employees, contractors, or third-party collaborators, across all repositories and services.

Principles. Reviews must focus on the code and its outcomes, not the individual. Feedback should be specific, actionable, and evidence-based. Reviewers and authors must presume good intent, communicate clearly, and document decisions for traceability. Urgent fixes require the same professionalism as routine work.

Roles and responsibilities. Authors are responsible for small, logically scoped changes, clear descriptions of context and intent, and inclusion of tests and documentation updates. Reviewers are responsible for timely, good-faith review against defined standards, asking clarifying questions before rejecting approaches, and suggesting concrete alternatives where possible. Both parties share responsibility for civility and resolution of disagreements.

Standards and criteria. Reviews assess correctness, security, performance, readability, test coverage, maintainability, compliance with style and architecture guidelines, and compatibility with backward-compatibility and migration policies. Blocking comments should be tied to a defined standard or risk. Non-blocking comments should be framed as suggestions and may be deferred to follow-up tasks where appropriate.

Communication norms. Use plain, respectful language and avoid sarcasm, labels, or personal judgments. Prefer “what” and “why” over “who.” Provide rationale and, where helpful, point to references or examples. If tone becomes tense, pause and escalate to asynchronous written rationale or a short live discussion moderated by a neutral engineer.

Process expectations. Authors should include a concise summary, context links to issues or designs, and test evidence. Reviewers should acknowledge within the agreed service-level window and either complete the review or set expectations for completion. Large changes should be broken into incremental reviews. For trivial nits, batch comments to avoid notification noise. Use draft and suggestions features to streamline acceptance. After approval and merge, authors should close the loop on any deferred items by ticketing and linking.

Quality and safety. No code merges without required approvals, passing checks, and security scans unless a documented emergency procedure is invoked, with a retrospective required within the next working day. Sensitive code (security, privacy, cryptography, payments, safety-critical systems) requires specialist review. Prohibit sharing of sensitive logs, secrets, or personal data in comments.

Disagreement and escalation. If author and reviewer cannot agree, first consult standards and architecture documents. Failing that, escalate to the designated code owner or a specified technical lead. Decisions should be recorded in the change log or design history for future reference.

Inclusion and mentorship. Reviews are opportunities to grow capability. Prefer questions like “Would you consider…” and explanations that help less-experienced contributors learn. Recognize contributions publicly and keep critical feedback private when it pertains to behavior rather than code.

Metrics and continuous improvement. Monitor review throughput, time-to-merge, rework rates, and defect escape rates to inform process tuning. Periodically refresh guidelines based on retrospectives and incident learnings.

Safety Committee Charter

Purpose. The Safety Committee (the Committee) provides oversight and guidance on health, safety, and environment matters to protect employees, contractors, customers, and the public, and to ensure compliance with applicable laws and company standards. The Committee supports a proactive culture of hazard identification, risk mitigation, and continuous improvement.

Authority. The Committee is authorized to request information from management, commission audits and risk assessments, access incident records, and retain external advisors as necessary. It operates under authority delegated by the Chief Executive Officer and reports to the Board or its designated committee where applicable.

Scope. The Committee covers occupational health and safety, contractor safety, product and service safety, environmental incidents that impact safety, emergency preparedness, and regulatory interactions related to safety. In regulated sectors, the Committee coordinates with quality, clinical, or reliability bodies to avoid overlap.

Composition. The Committee comprises cross-functional leaders from operations, facilities, engineering, human resources, legal, and compliance. The Chair is appointed by the CEO. At least one member should possess professional safety qualifications. Management designates a Secretary to maintain records.

Meetings and quorum. The Committee meets at least quarterly and ad hoc following serious incidents. A majority of members constitutes a quorum. The agenda includes review of leading and lagging indicators, incident trends, corrective actions, training status, audits, regulatory changes, and lessons learned.

Responsibilities. The Committee reviews safety policies and approves material updates; monitors key performance indicators such as total recordable incident rate, lost time rate, near-miss reporting, corrective action closure, and audit findings; oversees incident investigations to ensure root-cause analysis and timely remediation; ensures contractor and visitor safety programs are fit-for-purpose; reviews training plans and completion; evaluates changes with significant safety impact; and ensures emergency response and business continuity plans are current and tested.

Reporting. The Committee provides periodic reports to the executive team and Board on safety performance, material risks, significant incidents, enforcement actions, and corrective action status. It ensures transparency and promotes a just culture that encourages reporting and learning without fear of reprisal.

Document control and records. The Secretary maintains agendas, minutes, materials, and action logs for at least the statutory retention period or, absent regulation, no less than five years. Policies, procedures, and training materials are version controlled.

Annual evaluation. The Committee conducts an annual self-assessment of effectiveness, composition, and charter adequacy. Proposed changes to the charter are submitted for executive approval.

Investor Oversight Framework

Objective. This framework enables disciplined, value-focused oversight by the investor across the investment lifecycle, balancing active governance with management autonomy. It defines information rights, governance cadence, reserved matters, risk and compliance oversight, and performance monitoring.

Governance cadence. Establish a calendar for board meetings, committee sessions (audit and risk, compensation, safety or quality, technology), and monthly operating reviews. Define standing agendas, pre-read expectations, and decision logs. Ensure clear decision rights between the board, investor designees, and management.

Information rights. Formalize timely access to monthly financials, operating KPIs, liquidity reports, covenant compliance, customer and pipeline metrics, human capital dashboards, safety and quality indicators, cyber and privacy posture, and material litigation updates. Set standards for data definitions and ensure a single source of truth.

Reserved matters and approval matrix. Define actions requiring investor or board approval, including annual budgets, material deviations from plan, capital expenditures above thresholds, debt incurrence or amendments, M&A, divestitures, material commercial contracts, changes to auditor, adoption or amendment of key policies, and compensation plans for executives. Publish a clear RACI so management understands the escalation path and timelines.

Risk, compliance, and ethics. Require adoption and periodic certification of core policies (code of conduct, anti-bribery and corruption, sanctions, antitrust, data privacy and security, trade controls, whistleblowing, safety). Ensure incident reporting and investigation protocols are robust, with quarterly reporting of allegations, outcomes, and remedial actions. Mandate minimum compliance training and track completion.

Performance management. Define a value-creation plan with milestones, owners, and metrics. Use a consolidated dashboard to monitor revenue growth, gross margin, opex discipline, cash conversion, churn/retention, NPS or equivalent quality metrics, talent health, and major program delivery. Tie management incentive plans to measurable outcomes and clawbacks for misconduct or financial restatements where lawful.

Audit and controls. Require annual financial audits, internal controls maturity assessments, and targeted reviews of high-risk areas such as revenue recognition, procurement, inventory, and IT general controls. Track remediation with dated action plans. For leveraged structures, monitor borrowing base and collateral audits.

Technology and data. Set expectations for cybersecurity frameworks, incident response, disaster recovery, change management, data governance, and AI/ML risk management where applicable. For critical systems changes, require pre-implementation risk review and post-implementation validation.

ESG and sustainability. Align on material ESG topics for the sector and jurisdiction. Define a limited set of metrics for board oversight, including safety performance, greenhouse gas intensity where relevant, diversity metrics, and ethics indicators. Avoid reporting burdens unlinked to value or compliance.

Communications and escalation. Establish protocols for prompt notification of material events, including covenant breaches, significant incidents, cyber events, regulatory inquiries, and key-person changes. Define escalation paths to investor representatives and legal counsel and document post-mortems and lessons learned.

Exit readiness. From year one, maintain data hygiene, legal entity rationalization, IP assignments, and contracts repositories to facilitate refinancing or exit. Periodically test the equity story, run quality-of-earnings readiness, and address diligence gaps.

Deal-Term Integration Matrix

The following matrix maps key definitive agreement provisions to Day 1 and post-close integration actions, owners, and control evidence. Tailor columns and entries to the specific deal and industry.

Term/Provision	Risk/Obligation	Day 1 Actions	Post-Close Integration Actions	Owner	Evidence/Control	Timing
Financial statements and earn-out mechanics	Misstated baselines or disputes over earn-out; manipulation risk	Freeze baseline definitions and circulate accounting policy memo; establish data segregation and read-only snapshots	Implement governance for adjustments, independent review of metrics, dispute resolution playbook	CFO/Controller	Signed accounting policy memo; data snapshots; reconciliation logs	Day 1; monthly thereafter
Purchase price adjustment (NWC, debt, cash)	Working capital disputes; definitions gaps	Lock cut-off procedures; confirm calculation templates; designate dispute lead	Standardize closing balance sheet policies; schedule independent tie-outs	Finance; Legal	Closing binders; tie-out package; variance analyses	Day 1 to +90
Transition services agreement (TSA)	Service gaps; stranded cost risk	Validate service catalog, SLAs, exit criteria; stand up TSA governance	Build stand-alone capabilities; TSA reduction plan and cost tracking	IMO; IT; HR; Finance	TSA tracker; service credits; exit sign-offs	Day 1; weekly cadence
Regulatory approvals and commitments	Post-closing conduct restrictions; hold separate	Issue compliance instructions; implement information barriers and clean teams	Monitor commitments, periodic certifications,	Legal; Compliance	Clean team protocols; certification logs	Day 1; per regulator cadence

			divestiture milestones tracking			
Non-compete and non-solicit	Talent flight risk; restricted growth vectors	Communicate boundaries to go-to-market and recruiting; set CRM restrictions	Periodic audits of hiring and marketing territories; exception approvals	Legal; Sales Ops; HR	Training records; CRM rule sets; audit logs	Day 1; quarterly
IP assignments and licenses	Breaks in chain of title; use limitations	Confirm assignment filings and license effectiveness; freeze changes	Consolidate IP docket; remediate gaps; standardize OSS compliance	Legal; Engineering	Filing receipts; IP asset register; OSS SBOM	Day 1; +180
Data privacy and security covenants	Breach notification and security standards	Enforce access controls and MFA; segregate high-risk data; adopt breach playbook	Harmonize policies; complete security uplift plan; conduct tabletop exercises	Security; IT; Legal	Access logs; policy acknowledgments; tabletop reports	Day 1; semiannual
Employee matters (benefits, retention, TUPE)	Flight risk; benefit parity; works council	Execute retention grants; issue communications; complete required consultations	Benefits harmonization; policy alignment; organization design	HR; Legal	Comms plan; consultation minutes; signed plan docs	Day 1; +180
Material contracts consents	Termination risk; step-in failures	Confirm critical consents and interim performance; initiate change notices	Renegotiate unfavorable terms; novate where needed	Legal; Procurement; Sales	Consent tracker; executed novations; clause library	Day 1; +120

Tax covenants and elections	Straddle period risk; elections timing	Lock go-forward tax calendar; assign compliance responsibilities	Implement transfer pricing, indirect tax registrations, entity alignment	Tax	Tax calendar; filings; intercompany agreements	Day 1; annual cycle
Environmental, health, and safety	Legacy liabilities; operational continuity	Site access controls; incident reporting alignment; interim PPE standards	Integrate EHS management systems; complete corrective actions	EHS; Ops	Audit reports; CAPA logs; training records	Day 1; +365
Litigation and claims	Adverse outcomes; preservation failures	Issue legal holds; update counsel of record; align settlement authority	Quarterly docket review; integrate matter management	Legal	Hold notices; matter list; authority matrix	Day 1; quarterly
Customer and channel communications	Churn risk; misaligned messaging	Approve customer comms; stabilize service levels; protect SLAs	Harmonize terms; define cross-sell rules; monitor NPS	Sales; CS; Legal	Comms artifacts; SLA dashboards; NPS trend	Day 1; +180
Governance and reporting	Fragmented visibility; missed covenants	Establish integration management office and reporting cadence	Transition to steady-state KPI dashboards and board reporting	IMO; FPA	Playbooks; dashboards; action logs	Day 1; +90

Usage notes. Prior to close, pre-populate the matrix with the negotiated definitive agreement clauses and disclosure schedule items. At signing, assign named owners and define evidence artifacts. At close, begin cadence reporting and variance tracking. Archive a copy with closing deliverables.