Beagle Security

Cybersecurity due diligence checklist

A detailed, evidence-led workbook for reviewing a target's security maturity before a transaction.

Use this workbook to: capture the evidence reviewed, identify gaps, and translate technical findings into material deal risks, remediation follow-up, and decision-ready reporting.

Deal details

Target company	
Review date	

How to use it

- Collect the supporting records listed in the evidence column before marking an item complete.
- Validate documentation with engineering, DevOps, and security stakeholders; capture any mismatch in the follow-up field.
- Use scans and penetration testing to validate material vulnerability and exploitability claims.

Core evidence to collect

- Security policies, architecture diagrams, compliance documentation, and prior security assessments.
- Breach disclosures, audit logs, past incident records, root-cause analysis, and remediation timelines.
- Access and identity review material, vulnerability scan results, and penetration-test findings.
- Cloud and infrastructure documentation, data flows, and records of important integrations and third parties.

Application security

Validate the target's application and API exposure and authentication design.

Review check	Evidence to request / review	Status
Obtain the latest automated DAST and SAST results.	Record test date, scope, severity breakdown, and whether critical findings are still open.	☐ Yes ☐ N/A
Review critical CVEs and unresolved application vulnerabilities.	Ask for the remediation status, supporting evidence, and any accepted-risk decision.	☐ Yes ☐ N/A
Identify exposed APIs and internet-facing application endpoints.	Review the available endpoint or API inventory and compare it with test results.	☐ Yes ☐ N/A
Assess the application's authentication mechanisms.	Review the authentication design and evidence of testing for weak authentication paths.	☐ Yes ☐ N/A
Assess the maturity of secure development processes.	Review how security findings enter engineering work and how remediation is tracked.	☐ Yes ☐ N/A

Red flag focus: Critical CVEs, exposed APIs, or weak authentication.

Why it matters: These issues can affect customer data safety and product reliability.

Material findings

Cloud security

Review cloud access controls, visibility, and known configuration exposure.

Review check	Evidence to request / review	Status
Review IAM roles and policies.	Look for evidence that permissions are deliberate and reviewed, especially for privileged access.	☐ Yes ☐ N/A
Confirm cloud logging coverage.	Identify which cloud accounts, services, and environments generate logs and where they are retained.	☐ Yes ☐ N/A
Review recent cloud misconfiguration scan results.	Record the scan scope, most recent run date, and unresolved findings.	☐ Yes ☐ N/A
Identify publicly exposed services and open ports.	Confirm whether public access is required and document the business owner for each exception.	☐ Yes ☐ N/A
Review unrestricted IAM permissions.	Record broad privileges, their owners, and whether compensating controls exist.	☐ Yes ☐ N/A

Red flag focus: Open ports, unrestricted IAM permissions, or missing logs..

Why it matters: Cloud misconfigurations can create material exposure and are a major source of modern breaches.

Material findings

Infrastructure & network

Assess whether network design and patching reduce the risk of compromise.

Review check	Evidence to request / review	Status
Review network segmentation.	Use architecture diagrams to identify separation between critical systems, environments, and user access paths.	☐ Yes ☐ N/A
Review firewall rules.	Confirm that allowed traffic is intentional and that exceptions are documented.	☐ Yes ☐ N/A
Assess patch cadence.	Request evidence of how updates are identified, prioritized, and applied.	☐ Yes ☐ N/A
Identify legacy technology and unsupported operating systems.	Record where they remain in use and whether an upgrade or retirement plan exists.	☐ Yes ☐ N/A
Review device security hardening.	Confirm the target can explain its baseline approach to endpoint and system hardening.	☐ Yes ☐ N/A

Red flag focus: Legacy technology, flat networks, or unsupported operating systems.

Why it matters: They increase the likelihood of lateral movement and ransomware impact.

Material findings

Data protection

Understand how sensitive data is protected, retained, and recovered.

Review check	Evidence to request / review	Status
Verify encryption standards for sensitive data.	Record where encryption applies and whether any sensitive data is unencrypted.	☐ Yes ☐ N/A
Review key management practices.	Identify where keys are stored and who can manage or access them.	☐ Yes ☐ N/A
Review data handling practices.	Trace how sensitive data is collected, processed, stored, and shared.	☐ Yes ☐ N/A
Review data retention policies.	Confirm documented retention expectations and how they are applied in practice.	☐ Yes ☐ N/A
Verify backup and recovery procedures.	Request evidence that backups are reliable and recovery procedures have been considered.	☐ Yes ☐ N/A

Red flag focus: Unencrypted sensitive data or weak key storage.

Why it matters: Data protection gaps are directly tied to compliance exposure and breach impact severity.

Material findings

Identity & access management

Determine whether access to systems and data is appropriately authenticated, governed, and limited.

Review check	Evidence to request / review	Status
Verify MFA enforcement.	Confirm which users, systems, and access paths are protected by MFA and note exceptions.	☐ Yes ☐ N/A
Review role-based access control (RBAC).	Assess whether roles are defined and access is allocated according to job needs.	☐ Yes ☐ N/A
Review least-privilege access practices.	Identify high-privilege access and evidence that it is limited and reviewed.	☐ Yes ☐ N/A
Assess service account governance.	Document owners, purpose, permissions, and review expectations for service accounts.	☐ Yes ☐ N/A
Identify shared and orphaned accounts.	Record whether these accounts exist, who owns them, and whether a cleanup plan is active.	☐ Yes ☐ N/A

Red flag focus: Shared accounts, missing MFA, or privilege sprawl..

Why it matters: Identity weaknesses are a primary path to account takeover and internal misuse.

Material findings

Incident response

Assess whether the target can detect, investigate, and remediate security incidents in a repeatable way.

Review check	Evidence to request / review	Status
Review the incident response plan.	Confirm it exists, names accountable roles, and describes a repeatable response workflow.	☐ Yes ☐ N/A
Assess detection tooling.	Identify the tools used to detect and investigate suspicious activity.	☐ Yes ☐ N/A
Review historical incident logs and breach disclosures.	Request relevant records and look for recurring patterns or unresolved issues.	☐ Yes ☐ N/A
Review past incident remediation practices.	For material incidents, check whether root causes and remediation timelines were documented.	☐ Yes ☐ N/A
Validate operational visibility through stakeholder interviews.	Ask engineering, DevOps, and security leaders to explain how incidents are identified and escalated.	☐ Yes ☐ N/A

Red flag focus: Lack of procedures, poor visibility, or unresolved incidents.

Why it matters: This can point to hidden liabilities and a lack of readiness for future incidents.

Material findings

Vendor & supply chain risk

Understand the exposure introduced by external providers, APIs, SaaS platforms, and outsourced services.

Review check	Evidence to request / review	Status
Identify third-party APIs and integrations.	Request a list of material API dependencies and the systems or data they connect to.	☐ Yes ☐ N/A
Identify SaaS dependencies and outsourced services.	Document the providers that are important to the target's operations or data handling.	☐ Yes ☐ N/A
Review available third-party risk assessments.	Check whether material vendors have been reviewed and whether high-risk findings are documented.	☐ Yes ☐ N/A
Identify high-risk vendors.	Record why each vendor is high risk and the target's mitigation or monitoring approach.	☐ Yes ☐ N/A
Confirm the ownership of vendor review activities.	Identify the person or team responsible for assessing and reassessing third parties.	☐ Yes ☐ N/A

Red flag focus: High-risk vendors or no vendor reviews.

Why it matters: Third parties expand the attack surface and can increase the compliance burden.

Material findings

Compliance & governance

Validate whether stated compliance alignment is supported by real operational controls and records.

Review check	Evidence to request / review	Status
Validate the target's SOC 2 posture.	Request the relevant report or supporting compliance documentation and note identified gaps.	☐ Yes ☐ N/A
Validate the target's ISO 27001 posture.	Request available certification or program documentation and evidence of the underlying controls.	☐ Yes ☐ N/A
Review GDPR posture.	Request relevant privacy documentation, including data processing arrangements and records of processing activities where applicable.	☐ Yes ☐ N/A
Review HIPAA posture where applicable.	Request available HIPAA records and evidence of relevant safeguards.	☐ Yes ☐ N/A
Compare claimed certifications with operational controls.	Use interviews and evidence review to determine whether controls operate in practice, not only on paper.	☐ Yes ☐ N/A

Red flag focus: Unverifiable certifications or major control gaps.

Why it matters: Compliance gaps can affect customer trust and market eligibility.

Material findings

DevSecOps & SDLC

Assess whether security is built into the delivery process or relies on late, manual intervention.

Review check	Evidence to request / review	Status
Review CI/CD security controls.	Identify security checks in the delivery pipeline and how findings are handled.	☐ Yes ☐ N/A
Review code review practices.	Confirm whether code changes receive review and how security-relevant changes are escalated.	☐ Yes ☐ N/A
Assess secrets management.	Determine how secrets are stored, accessed, rotated, and kept out of source code.	☐ Yes ☐ N/A
Identify hardcoded secrets.	Review evidence from code review, scanning, or past findings and record any unresolved exposure.	☐ Yes ☐ N/A
Assess the security control coverage in the pipeline.	Identify whether the delivery process lacks controls or depends on individual practice.	☐ Yes ☐ N/A

Red flag focus: Hardcoded secrets or no security controls in the pipeline.

Why it matters: These signs indicate operational immaturity and may increase long-term remediation cost.

Material findings

Executive risk summary

Use this final page to convert the completed checklist into a concise decision record.

Material finding	Business impact	Risk level	Next step