Beagle Security

IT security audit checklist

A companion to our IT security audit guide. Same nine categories, with the practical detail behind every item: why it matters and what good looks like.

Work through each section against your own environment, or use it as a starting agenda for your next internal or external audit.

Governance and policies

- [ ] **Review security policies, standards, and procedures for completeness and currency**

  Policies that haven't been touched since the last audit cycle rarely reflect how the business actually operates today. Check that they cover current cloud providers, remote work arrangements, and any new product lines, not just the infrastructure that existed when they were written.

- [ ] **Evaluate security governance structure and reporting relationships**

  Security decisions get made faster, and stick better, when there's a clear line from the security function to leadership. Confirm who owns security outcomes, who they report to, and whether that person has the authority to enforce fixes, not just recommend them.

- [ ] **Assess security awareness and training programs**

  A single annual training video rarely changes behavior. Look for training that's role-specific, engineers need different guidance than finance, and reinforced with periodic phishing simulations rather than a once-a-year checkbox.

- [ ] **Verify documentation of security controls and procedures**

  A control that only exists in someone's head doesn't survive that person leaving. Confirm controls are documented well enough that a new hire or an external auditor could follow them without a walkthrough.

- [ ] **Review security strategy alignment with business objectives**

  Security work that isn't tied to what the business is actually trying to do gets deprioritized the moment budgets tighten. Check that the security roadmap references the same growth, compliance, or product goals leadership is already tracking.

Risk management

- [ ] **Examine risk assessment methodologies and documentation**

  A risk register that hasn't been updated since it was created isn't tracking risk, it's archiving it. Confirm the methodology accounts for new assets, new vendors, and new attack techniques, and that each assessment is dated and owned.

- [ ] **Evaluate risk treatment plans and their implementation status**

  Identifying a risk and doing something about it are two different milestones. For each open risk, check whether there's an assigned owner, a treatment plan, and a target date, not just a severity rating sitting in a spreadsheet.

- [ ] **Review processes for identifying and addressing new security risks**

  New risks show up between audit cycles, a new integration, a new region of operation, a new class of vulnerability. Confirm there's a standing process for capturing these as they appear, not a mechanism that only resets once a year.

- [ ] **Assess third-party risk management procedures**

  Vendors and subprocessors carry your data, which means their risk becomes your risk. Check that vendor risk assessments happen before onboarding, not after an incident forces the question.

- [ ] **Verify business continuity and disaster recovery plans**

  A recovery plan that's never been tested is a hypothesis, not a plan. Confirm recovery time objectives and recovery point objectives are documented, and that the plan has actually been rehearsed.

Access control and identity management

- [ ] **Review user provisioning and deprovisioning processes**

  Access that isn't revoked promptly when someone leaves is one of the most common findings in any audit. Confirm deprovisioning happens the same day as offboarding, and check for accounts that should have been closed months ago.

- [ ] **Evaluate password policies and implementation**

  Length and complexity rules matter less than whether they're enforced technically, not just written in a policy document. Confirm enforcement happens at the identity provider level, and check for shared or service accounts that bypass it entirely.

- [ ] **Assess privileged access management controls**

  Admin and root accounts are the accounts attackers want most. Confirm privileged access is granted only when needed, time-limited where possible, and logged separately from standard user activity.

- [ ] **Verify multi-factor authentication implementation where appropriate**

  MFA on the front door doesn't help if it's missing on the admin panel, the cloud console, or the CI/CD system behind it. Confirm coverage extends to every system that can change production state, not just the ones users log into daily.

- [ ] **Review user access rights and separation of duties**

  Access tends to accumulate as people change roles and rarely gets cleaned up on the way. Check for users still holding permissions from a previous role, and confirm no single person can both request and approve a sensitive change.

- [ ] **Examine session management controls**

  Long-lived sessions and tokens that never expire give an attacker a wider window if credentials are ever compromised. Confirm session timeout, token rotation, and revocation on logout are enforced consistently across applications, and consider testing this behavior directly through authenticated scans rather than assuming it holds up under real use.

Network security

- [ ] **Evaluate network architecture and segmentation**

  A flat network means one compromised device can reach everything else on it. Confirm production, staging, and internal systems sit in genuinely separate network segments, not just separate folders on the same subnet.

- [ ] **Review firewall configurations and rules**

  Firewall rulesets tend to accumulate exceptions over time and rarely get cleaned up. Check for rules that were added for a project that no longer exists, and confirm the default posture is deny, not allow.

- [ ] **Assess wireless network security controls**

  Guest networks that share infrastructure with corporate Wi-Fi are a common weak point. Confirm encryption standards are current and that guest traffic is fully isolated from internal systems.

- [ ] **Verify remote access security measures**

  Remote access has expanded for most organizations, and so has the attack surface that comes with it. Confirm VPN or zero-trust access is required for anything touching production, and that it's tied to individual identity rather than shared credentials.

- [ ] **Review network monitoring and intrusion detection capabilities**

  Detection only helps if someone is watching it. Confirm alerts from monitoring tools have an owner and a response process, not just a dashboard nobody checks.

- [ ] **Examine email and web filtering controls**

  Most attacks still start with a phishing email or a malicious link. Confirm filtering is tuned to catch known-bad patterns without generating so many false positives that people start ignoring the warnings.

Systems and applications security

- [ ] **Review system hardening practices**

  Default configurations are built for ease of setup, not security. Confirm unnecessary services are disabled and that hardening baselines are applied consistently across servers, not just the ones someone remembered to configure.

- [ ] **Assess patch management processes**

  A known vulnerability with an available patch is one of the easiest things for an attacker to exploit, and one of the easiest things to fix. Confirm there's a defined window for applying critical patches, and check how long the oldest unpatched critical vulnerability has been open.

- [ ] **Evaluate change management procedures**

  Changes made without review are a common source of outages and security gaps alike. Confirm production changes go through a documented approval step, even for small fixes, and that there's a rollback plan for anything touching customer-facing systems.

- [ ] **Review secure development practices for in-house applications**

  Security bolted on after release costs more to fix than security built in from the start. Confirm developers have access to secure coding guidelines and that code is reviewed for security issues, not just functionality, before it ships.

- [ ] **Verify vulnerability management programs**

  A scan that runs once a quarter misses everything that changed in between. Automated, continuous testing against your web applications and APIs, the kind Beagle Security runs, surfaces new vulnerabilities as code ships rather than waiting for the next scheduled window.

- [ ] **Assess database security controls**

  Databases hold the data attackers actually want, which makes them a priority target. Confirm access is restricted to service accounts with least privilege, and that sensitive fields are encrypted rather than stored in plain text.

Data protection

- [ ] **Review data classification and handling procedures**

  Not all data carries the same risk, and treating it that way wastes effort protecting low-value data while under-protecting the sensitive kind. Confirm a classification scheme is in place and that handling rules actually differ by classification level.

- [ ] **Evaluate data encryption implementation for data at rest and in transit**

  Encryption enabled somewhere in the stack isn't the same as encryption enforced everywhere sensitive data travels or sits. Confirm TLS is enforced on every endpoint, and that databases and backups are encrypted at rest, not just the primary datastore.

- [ ] **Assess data loss prevention controls**

  Data doesn't only leave through a breach, it leaves through a misconfigured share, an email attachment, or an export nobody tracked. Confirm there are controls, technical or procedural, over how sensitive data can leave your environment.

- [ ] **Review data retention and disposal practices**

  Keeping data longer than needed only increases what's exposed if something goes wrong. Confirm retention periods are defined by data type and that disposal actually happens on schedule, not just gets scheduled.

- [ ] **Verify backup procedures and security of backups**

  Backups are a favorite target for ransomware precisely because they're often less protected than production. Confirm backups are encrypted, access to them is restricted, and restoration has actually been tested recently.

Physical security

- [ ] **Evaluate physical access controls to facilities and data centers**

  Even with most infrastructure in the cloud, physical access to offices and any remaining on-premises equipment still matters. Confirm access is logged, badges are deactivated promptly on offboarding, and shared or unmanaged entry points are addressed.

- [ ] **Review environmental controls (power, cooling, fire suppression)**

  Environmental failures cause outages just as effectively as cyberattacks do. Confirm critical infrastructure has documented environmental safeguards and that they're tested, not just installed.

- [ ] **Assess physical media handling and disposal procedures**

  A decommissioned hard drive or an old backup tape can carry as much sensitive data as an active server. Confirm media is wiped or destroyed through a verified process before disposal.

- [ ] **Verify monitoring of physical access and security incidents**

  Access logs that nobody reviews provide a record after the fact, not protection in the moment. Confirm physical security events have a defined review and escalation process.

Incident management

- [ ] **Review incident response procedures and capabilities**

  A plan that exists only as a document nobody has read isn't a plan during an actual incident. Confirm the team knows the plan exists, knows their role in it, and has practiced it at least once.

- [ ] **Assess security monitoring and detection mechanisms**

  Response time depends entirely on how quickly an incident is detected in the first place. Confirm monitoring covers the systems that matter most, and that alerts reach someone who can act on them at any hour.

- [ ] **Evaluate incident reporting and escalation processes**

  Confusion about who to notify and when costs valuable time during an active incident. Confirm escalation paths are clear, including when legal, customers, or regulators need to be looped in.

- [ ] **Review lessons learned processes following security incidents**

  An incident that doesn't change anything afterward is likely to happen again. Confirm there's a structured post-incident review that produces concrete follow-up actions, not just a summary.

- [ ] **Verify integration with business continuity plans**

  Incident response and business continuity are often written by different teams and never actually tested together. Confirm the two plans reference each other, so a major incident doesn't leave a gap between containing the threat and keeping the business running.

Compliance and third-party management

- [ ] **Verify compliance with applicable regulations and standards**

  Compliance status can drift between formal audits as systems and vendors change. Confirm someone is tracking your posture against frameworks like SOC 2, HIPAA, or PCI DSS on an ongoing basis, not just in the weeks before the audit.

- [ ] **Review vendor security assessment processes**

  A vendor with weak security practices becomes your weak point the moment they touch your data. Confirm new vendors go through a security review before onboarding, scaled to the sensitivity of what they'll access.

- [ ] **Evaluate contractual security requirements for service providers**

  Verbal assurances from a vendor don't hold up if something goes wrong. Confirm contracts specify security obligations, breach notification timelines, and audit rights, not just service levels.

- [ ] **Assess ongoing vendor security monitoring procedures**

  A vendor that passed review a year ago may not still meet the same bar today. Confirm there's a recurring check-in on vendor security posture, and that evidence such as OWASP-mapped pentest reports gets refreshed on a schedule your auditors will accept, not treated as a one-time approval.

Put the systems and applications section into practice

Beagle Security runs agentic penetration tests against your web applications and APIs, including internal apps behind Cosmog tunneling, with business logic testing and OWASP-mapped reports built in. Start a 14-day free trial with Advanced plan features, no credit card required, or take the interactive demo for a self-guided look first.