TUAN SECURITY GROUP

The Founder’s Guide to Passing Enterprise Security Reviews

The Security Foundation Every Startup Needs Before Enterprise Customers Start Asking Questions

You built the product. You found product-market fit. Customers are starting to take notice. Then one day, a large customer sends over a security questionnaire.

- Do you have a security program?
- How do you manage employee access?
- How do you protect customer data?
- Do you have an incident response plan?
- Are your vendors secure?
- Can you prove your controls are working?

For many startups, this is where growth slows down — not because the company is not secure, but because security was never built intentionally.

Enterprise customers do not expect a 20-person startup to have the same security program as a Fortune 500 company. They do expect you to have the fundamentals in place.

The companies that move through security reviews quickly are not the ones with the most tools. They are the ones that built the right foundation early. This guide covers the security areas every startup should address before security becomes a blocker to growth.

1. Build Customer Trust Before They Ask

The first question enterprise customers are really asking is: *"Can we trust this company with our data?"* Before a customer signs a contract, they want confidence that you understand your security responsibilities.

Your company should have clear answers around:

- What customer data you collect
- Where that data is stored
- Who can access it
- How access is controlled
- How security incidents are handled

Start with the basics:

- ☐ Create a security page that explains your security approach
- ☐ Maintain customer-facing documentation: Privacy Policy, Terms of Service, Data Processing Agreement (DPA), and Security overview documentation

FOUNDER CHECKPOINT

"If a Fortune 500 customer asked us how we protect their data tomorrow, would we have a confident answer?"

2. Control Who Has Access to Your Business

Startups move fast. New employees join. Contractors help build the product. New tools get added every month. Over time, access becomes messy.

The question is simple: **Who has access to your most important systems, and should they still have it?**

Important systems include:

- Cloud infrastructure
- Source code repositories
- Customer databases
- Business applications & internal tools

Your foundation should include:

- Knowing what systems your company uses
- Understanding who has access
- Giving employees only the access they need
- Removing access when someone leaves
- Reviewing access regularly

Strong authentication matters: For important systems, move beyond passwords and basic MFA when possible by using stronger options like passkeys or security keys.

FOUNDER CHECKPOINT

"If someone left the company today, could we confidently remove their access everywhere?"

3. Create Simple Employee Access Processes

Security does not have to mean slowing your team down. You do not need expensive enterprise identity tools to build good processes. You need consistency.

When someone joins:

- ☐ They request access
- ☐ Their manager approves the need
- ☐ The appropriate person grants access
- ☐ The request is documented

When someone leaves:

- ☐ Accounts are disabled
- ☐ Application access is removed
- ☐ Permissions are revoked
- ☐ Company devices are recovered
- ☐ Completion is documented

A simple ticketing process can work. What matters is proving: **Someone requested it. Someone approved it. Someone completed it.**

4. Secure the Devices That Access Your Company

Your employees' laptops are often the front door into your business. A compromised device can become a path into customer data, internal systems, source code, and cloud environments.

Your baseline should include:

- ☐ Device encryption
- ☐ Screen lock requirements
- ☐ Automatic updates
- ☐ Strong authentication
- ☐ Endpoint protection

You do not need the same security stack as a bank. You need security controls that match your company's risk and customer expectations.

5. Protect Your Most Valuable Data

Not every piece of data deserves the same level of protection. Start by identifying your company's crown jewels (Customer information, production databases, source code, API keys, financial information).

Understand:

- Where important data exists & who can access it
- How it is protected & how unnecessary data is removed

The goal is simple: Protect the information that would create the biggest impact if compromised.

FOUNDER CHECKPOINT

"If our largest customer asked how we protect their data, could we explain it clearly?"

6. Have Backups You Can Actually Recover From

Everyone talks about backups. Few companies test whether they work. A real backup strategy answers: *What is backed up? How often? Who manages it? How quickly can we recover?*

Your company should have backups for:

- ☐ Customer data & databases
- ☐ Critical files & cloud environments
- ☐ Regular recovery testing

Because a backup you cannot restore is not a backup plan.

7. Focus on the Risks That Matter Most

Every startup has vulnerabilities. The goal is not to eliminate every possible risk. The goal is knowing which risks could actually impact your business.

Prioritize issues involving:

- Production systems & customer-facing applications
- Sensitive customer data & critical vulnerabilities

A low-risk issue in a testing environment is very different from a critical issue affecting customer data. Security maturity is about prioritization.

8. Understand Your Technology Vendors

Your security extends beyond your own company. Your vendors may have access to customer information, internal systems, and business data.

Know & Review:

- Which vendors you rely on and what information they handle
- Review vendors for security certifications, SOC 2 reports, security incidents, and data protection practices

Enterprise customers will evaluate your vendors. You should too.

9. Be Ready When Security Incidents Happen

The question is not whether something will happen. The question is: *Will your team know what to do when it does?*

A strong incident response plan defines:

- How incidents are detected & who is responsible
- How threats are contained & how systems are recovered
- How customers are notified & how lessons are documented

The worst time to create an incident plan is during an incident.

10. Make Sure Your Business Can Recover

Customers want confidence that your company can keep operating when things go wrong (cloud provider outages, accidental data deletion, loss of critical employees, business disruptions).

Build:

- Critical system inventory & recovery procedures
- Business continuity plans & disaster recovery testing

Resilience is part of security.

11. Keep Security Ready as You Scale

SOC 2 and enterprise security reviews are not one-time projects. The companies that scale successfully make security part of how they operate.

Maintain consistently:

- ☐ Access reviews & vendor reviews
- ☐ Security training & risk assessments
- ☐ Vulnerability management & policy updates

Security maturity is built through consistency.

The Reality for Growing Startups

Most founders do not need more security tools. They need clarity. They need to know:

- What matters first & what customers actually expect
- What auditors will look for
- Which tools are necessary vs. unnecessary
- How to build security without slowing down engineering

The startups that win enterprise customers are not the ones that panic when security questions arrive. They are the ones that prepared before they were asked.

Need help building your security foundation?

We help early-stage companies build practical security programs that prepare them for enterprise customers, SOC 2 readiness, and long-term growth.

Email: john@tuansecuritygroup.com