



Preparing for Technical Due Diligence

TechCXO Technical Due
Diligence Process Overview

— 2024

Technical Due Diligence

Critical for every business transaction involving tech M&A, investments, and partnerships. **An in-depth evaluation of technology strategy, assets, systems, security, team, roadmap, and development process to identify risks, weaknesses, and opportunities.**



Leverage TechCXO Product & Technology Experts



What is an investor / acquirer looking for?

RISK, RISK, RISK (and anything that might cost a lot of money later)

PRODUCT

Is there product-market fit and a clear plan for how to deliver needed value? Is there a solid roadmap?

ARCHITECTURE / CODE REVIEW

Is the application built in a solid and scalable way that is supportable? Does the company fully own the code?

TEAM ASSESSMENT

Is there a solid team in place with strong leaders who can lead at the next level? Can the team scale?

SECURITY

Is there anything that could potentially be a threat to the business from a breach or denial of service perspective?

HOSTING / DEPLOYMENT

Is the application hosted in a secure manner that facilitates significant scale and simple deployment.

IT

Is there anything IT-related that will make it difficult or costly to integrate and scale the business?



What to Expect

Probably requires around 1-2 days of effort, all in. The overall process is around 3-4 weeks.



You will likely receive a detailed list of questions to answer covering the areas outlined above.



Kick-off call to meet the team, walk through the diligence process, and identify follow-up discussions. Also, will want access to code.



Follow-up discussions in each of the areas outlined - could be separate or one long session. Will drill in on gaps or answers provided.



May need follow-up discussion(s) to clarify findings or could be handled by email.

Technical Assessment

ARCHITECTURE & CODE REVIEW

Using the Architectural and Tradeoff Analysis Method (ATAM), review architecture and code quality across five standard factors.

OPEN SOURCE ASSESSMENT

Verify company software rights and investigate open-source distribution restrictions and/or known security vulnerabilities.

DEVELOPMENT PROCESS

Understand the level of maturity for current product development workflows, design, quality control programs, and release processes.

DEVELOPMENT TEAM

Compare to high-performing team structures; evaluate team skills, capabilities, leadership gaps, and high-impact areas to consider post-transaction.

DEVOPS & HOSTING INFRASTRUCTURE

Ensure hosting environments are configured for scale and security; investigate evidence of best practices to ensure reliable code deployment.

Product Assessment

**STRATEGIC
ROADMAP
PLANNING**

**PRODUCT TEAM
STRUCTURE &
ROLES**

**CUSTOMER
EXPERIENCE**

**OFFER
COMPLETENESS &
MARKET-FIT**

**PRODUCT
LIFECYCLE
MANAGEMENT**

**PERFORMANCE
& METRICS**

Security Assessment

SECURITY ASSESSMENT LEVELS

TechCXO offers varying levels of Security Assessments, ranging from Quick Interview to full HIPAA or SOC2 Readiness Audit.

We typically start with an IG1 audit, following the Center for Internet Security (CIS) framework to measure safeguards for security hygiene.

CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7	CONTROL 03 Data Protection 14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12	CONTROL 05 Account Management 6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6	CONTROL 06 Access Control Management 8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8
CONTROL 07 Continuous Vulnerability Management 7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7	CONTROL 08 Audit Log Management 12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12	CONTROL 09 Email and Web Browser Protections 7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7
CONTROL 10 Malware Defenses 7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7	CONTROL 11 Data Recovery 5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5	CONTROL 12 Network Infrastructure Management 8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8
CONTROL 13 Network Monitoring and Defense 11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11	CONTROL 14 Security Awareness and Skills Training 9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9	CONTROL 15 Service Provider Management 7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7
CONTROL 16 Applications Software Security 14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14	CONTROL 17 Incident Response Management 9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9	CONTROL 18 Penetration Testing 5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

STANDARD IG1 ASSESSMENT

IT Health Assessment

TECHNOLOGY
SYSTEM
GOVERNANCE

TECHNOLOGY
SYSTEM ACCESS &
CONTROL

IT TEAM
STRUCTURE &
ROLES

ASSET
MANAGEMENT

IT & HELPDESK
PROCESS

Lessons from 200+ Projects

- Be prepared & be honest!
- Think about it from the buyer's perspective
- Let the technical team lead - CEO speaking for CTO is a red flag
- A problem is typically only a significant concern if there is no plan
- Nobody is going to steal your code - not giving code access is a red flag
- Treat it as an opportunity and not a threat