COMPLIANCE HEALTH CHECK GUIDE

A Strategic Self-Assessment for Growing Organizations

Turn compliance from a cost center into your competitive advantage.

Strong Cyber Solutions
strongcybersolutions.com

DRAFT v1.0

INTRODUCTION

Is Your Compliance Program a Strategic Asset or a Point-in-Time Project?

Many companies pursue compliance to check a box for a customer or an audit. They build a program that looks good on paper but crumbles under real-world scrutiny. This leads to failed enterprise sales, investor concerns, and costly remediation efforts later. A mature compliance program isn't about passing a single audit. It's about building a resilient, scalable system of governance that becomes a competitive advantage.

> *This guide is a self-assessment tool to help you gauge the maturity of your program. Answer these questions honestly to identify your strengths and, more importantly, your critical gaps.*

01 THE FOUNDATION

Access Control & Identity — The bedrock of your security.

1. **Centralized Management: Do you use a central identity provider (like Okta, Azure AD) to manage user access to your key applications?**

✓ MATURE	◑ DEVELOPING	○ INITIAL
All critical applications are managed via a central SSO provider.	Some applications use SSO, but many are still managed individually.	Access is managed manually and separately for each application.

2. **Password & Authentication Security: Is Multi-Factor Authentication (MFA) required for all access to production systems and sensitive applications?**

✓ MATURE	◑ DEVELOPING	○ INITIAL
MFA is enforced universally for all employees and contractors.	MFA is required for some, but not all, critical systems.	MFA is not consistently enforced.

3. **Principle of Least Privilege: Do you have a formal process for regularly reviewing user access and revoking it when no longer needed?**

✓ MATURE	◑ DEVELOPING	○ INITIAL
Automated, quarterly access reviews are assigned to managers and tracked for completion.	Access reviews happen, but they are manual and inconsistent.	There is no formal process for reviewing or revoking access.

02 THE FRAMEWORK

Policies & Risk Management — Your rules and how you apply them.

1. **Living Documentation: Are your security policies reviewed and updated at least annually, and actively used to guide employee behavior?**

✓ MATURE	◑ DEVELOPING	○ INITIAL
Policies are on a formal review cycle, and all employees are trained on them annually.	Policies exist but are rarely reviewed or referenced.	Policies are informal, incomplete, or non-existent.

2. Understanding Your Risk: Do you have a documented Risk Register that identifies your top security risks and a plan for mitigating them?

✓ MATURE	◑ DEVELOPING	○ INITIAL
A formal Risk Register is maintained, reviewed quarterly, and drives security priorities.	Risks have been identified informally, but are not tracked in a formal register.	There is no formal process for identifying or tracking risk.

3. Vendor Management: Do you have a process to assess the security of your critical third-party vendors (e.g., cloud provider, key SaaS tools)?

✓ MATURE	◑ DEVELOPING	○ INITIAL
All critical vendors are formally reviewed, and their compliance is tracked.	Some vendors are reviewed, but there is no consistent process.	Vendors are onboarded with little to no security review.

03 THE OPERATIONS

Proactive Security & Development — Security as an operational discipline.

1. Secure Development: Is security a part of your software development lifecycle (e.g., code reviews, dependency scanning)?

✓ MATURE	◑ DEVELOPING	○ INITIAL
Security testing and reviews are automated and required steps before code is deployed.	Developers are encouraged to write secure code, but there are no formal gates.	Security is an afterthought, addressed only after a product is built.

2. Incident Readiness: Do you have a documented Incident Response Plan, and has your team ever practiced it?

✓ MATURE	◑ DEVELOPING	○ INITIAL
A formal plan exists and is tested annually via tabletop exercises.	A plan exists on paper, but it has never been tested.	There is no formal plan; the team would have to improvise.

SCORING YOUR MATURITY

Tally your answers — count your Mature, Developing, and Initial responses per section.

MOSTLY "MATURE"	You have a strong foundation. The next step is to formalize this for enterprise-grade scrutiny and ensure it scales as you grow.
MOSTLY "DEVELOPING"	You have the right ideas but lack the process and consistency. You are at high risk of audit findings and security gaps as you scale. This is a critical inflection point.

MOSTLY "INITIAL"	Your compliance is likely ad-hoc and a significant business risk. A major breach or failed sales process is a real possibility. You need a strategic partner to build a program from the ground up.

YOUR NEXT STEP

This Health Check is a starting point. The real value comes from turning these insights into a strategic, actionable plan. A generic checklist won't address your unique technology stack, business model, or risk tolerance.

If you're ready to move from a reactive checklist to a proactive governance program — let's talk.

Book a complimentary 30-minute Governance Architecture Assessment

We'll review your results and help you build a roadmap that turns compliance from a cost center into your competitive advantage.

STRONG CYBER SOLUTIONS

strongcybersolutions.com