# The Security Journey Self-Assessment

TECHNICAL FRAMEWORK
MANAGED IT & CYBERSECURITY

Knowing your security starting point is crucial to becoming an impenetrable, security-first solution provider. Take this assessment to see which phase of the journey you're currently in.

Choose the answer that most closely aligns with your security practices today.

1. How would you describe your current security prowess?
   a. We have a desire to understand it but don't have the know-how.
   b. We've started digging into security and now need investments in time, talent, and treasure.
   c. We have a plan and a roadmap for every situation.
   d. We have good experience in security to share with others so we can fight this together.
2. How much are risk assessments part of your ongoing services?
   a. We do not currently perform risk posture assessments.
   b. We assess and discover vulnerabilities, but don't remediate beyond what our clients budget for.
   c. We do risk assessments for every client and follow up with a remediation plan and a timeline each time.
   d. Our clients' risks are continually assessed, remediated, and tested as part of our standard procedures.
3. What is your current approach to security with clients?
   a. We recommend solutions to our clients when they have an incident or we discover an issue.
   b. We've made sure every client has met our minimum requirements for security in today's threat landscape.
   c. We have solid security offerings with advanced features for greater protection.
   d. We offer an end-to-end strategic platform to deliver a comprehensive security offering.

4. What drives you to advance your security offering?

    a. Our clients' requests and expectations around what we're delivering.

    b. Our clients' willingness to spend money on advanced security.

    c. Our desire to put more focus on security protections.

    d. It's part of our strategic plan to be a security-focused solution provider.

5. How well are you able to monetize new security offerings?

    a. We are unable to monetize our security offerings.

    b. We have had some success monetizing it, but not consistently.

    c. We are adequately compensated for the responsibility of securing our clients' environment in today's threat landscape.

    d. We can charge a significant amount because of our superior delivery and execution.

6. What are your clients' expectations of your responsibilities as their service provider?

    a. They believe we own their security and are responsible if something happens.

    b. We have discussions about the ownership of security risks between both parties.

    c. There is mutual agreement on ownership of risk with all clients.

    d. We have a joint security risk management strategy with clear communication and boundaries.

7. What is your incident response plan made up of?

    a. Backups and cybersecurity insurance only

    b. Suggested incident response, disaster recovery, and business continuity plans

    c. Well defined incident response plan

    d. Well tested and communicated incident response plan

8. What is the current security prowess of your staff?

    a. No security expertise

    b. Training to develop expertise among resources

    c. A couple of in-house security experts

    d. Significant certified security experts on staff

9. What do your client conversations around security look like?

    a. We discuss it as a client brings it up.

    b. We are initiating security conversations with clients more frequently.

    c. We have regularly scheduled security conversations with clients.

    d. Security conversations are required for each of our clients.

10. What minimum cybersecurity standards do you require with clients?

    a. None

    b. Recommended minimum requirements

    c. Expected standards (or we may walk)

    d. Required standards (we walk if they’re not met)

Tally up the number of answers you have of each letter:

______________ “a” responses

______________ “b” responses

______________ “c” responses

______________ “d” responses

**Results:** The letter with the most responses corresponds with your current phase of the security journey.

### A – Clueless in Security

If you're in this phase, you're just getting started. Don't fret! Everyone started here at one point. Solution providers in this stage embody these qualities:

- Desire and recognize the need to implement security but don't know how.
- Pull together some security point products; fill a few gaps; call it security.
- Client assumes managed services include security. By default, you assume all the risk but don't make any additional revenue.
- Little or no proactive discussion. Some high-level conversation but nothing specific or strategic. Avoid the topic completely with some clients.

### B – Starting to Understand

If you're in this phase, you're starting to gain awareness and create plans. Solution providers in this stage embody these qualities:

- Aware and committed to invest time, treasure, and talent to get security implemented and done correctly.
- Use outside expertise. Table stakes security locked in. Evaluate processes and products to piece together a comprehensive offering.
- Solid security offering with advanced features. Provide user education. Begin charging for it. Unwilling to walk away from clients who don't adopt the security standard.
- Discuss what proper security planning and execution entails.

**C – Investing Time, Talent, and Treasure**
If you're in this phase, you're investing significantly in security becoming a part of the fabric of your operations. Solution providers in this stage embody these qualities:

- Security-first culture. Ask, "How will this change impact security?"
- Manage the security of data (accessibility and recoverability). Trained, dedicated security champion within the organization.
- Comprehensive security offering. Receive fair compensation for owning a large portion of the risk. A clear understanding that security is a shared responsibility.
- Security performance report provided quarterly along with ongoing planning to stay apprised of the new threat landscape.

**D – Unmovable, Security-First**
If you're in this phase, you've built mastery within your security practice that's worth sharing and with others in your community. Solution providers in this stage embody these qualities:

- Partner with the IT community to make everyone better. Realize security is a shared responsibility (vendors/partners/community/clients).
- Involved with and sharing openly with security communities and peers. Certified security professionals on staff.
- Create increased business value while giving back. Audited organizational security certification like CompTIA Security Trustmark+, SOC2, or ISO 27001.
- Clients understand regularly discussed security strategy, plan, budget, and execution. Share insights with industry peers and continue to educate the team.

**Mostly As, Bs, or Cs?** Set up some time with one of our security experts to learn how you can expand your offerings and provide more value for your clients—AND make more revenue.
Contact Us Today >>