

KEY QUESTIONS

to Ask When Selecting Information Security Providers



Introduction

By its very nature, information security requires a high level of trust. You need to be completely confident that a provider is honest and experienced and therefore capable of delivering the protection your organization requires. You also want assurance that a provider is giving you the contractual flexibility necessary for solid short- and long-term value. However, defining “trust”—and ferreting out the attributes that comprise it—is not easy. To help assess the trustworthiness of your current and/or prospective providers, pose the following questions and carefully consider the answer to each.

“ Be cautious of the seller-doer model. Recommended solutions may be best for the provider—not you. ”

Attribute #1: Intellectual Honesty

Many providers of information security consulting and outsourcing have agendas to sell related products and services. Such incentives may color their recommendations to you—resulting in an approach or solution that’s a bad fit, a bad value, or both. To determine if a provider is intellectually honest, ask:

1. **What is your service delivery model? How are your practitioners compensated (i.e., are they compensated on customer satisfaction and productivity, or do they also have incentives to sell more activities)? Do you have clear policies for separating sales and delivery?**

TIP: Watch for consultancies that use a “seller-doer” model, as these consultants are trained and compensated to continually sell more services—regardless of what’s best for your organization.

2. **Is your services team a division of a company that sells spam filtering, data encryption, database security assessment and testing, and/or other products and services?**

TIP: Watch for resellers that push you to purchase the products they resell; what’s best for them may not be best for you.

3. **Do you use certified practitioners who adhere to a code of ethics? How do you ensure that your practitioners are truly committed to information security as a professional discipline, much like law or medicine?**

TIP: Seek a provider that relies on certification and ethics as the backbone of its approach.

4. Are you experienced in delivering difficult security assessments and/or recommendations (when appropriate)? How do you ensure effective communication of such news throughout an organization—from the C-suite to the operations team?

TIP: Ask a provider to share specific examples of how it provided “tough love” news to previous clients.

Attribute #2: Experience

The market is awash in technical certifications. All of them sound impressive, but in the realm of information security, only two—CISM and CISSP—denote a true mastery of the discipline. Of course, being a certified subject-matter expert is only one requirement for being an experienced practitioner. The others include industry experience, a proven ability to mentor peers and clients, and regional acclaim as a business leader. Those four criteria constitute a very tall order—one that many providers are unable to deliver. To determine if a provider offers the right level of practitioners, ask:

1. Can you provide biographies of the people who will be deployed?

TIP: Review bios carefully to ensure that each practitioner offers information security certification, knowledge of your industry, a proven ability to mentor and coach, and a record of business achievement.

2. Has each individual already performed the type of work our organization needs? Can you provide personal references for your individual practitioners?

TIP: Experienced practitioners will not hesitate to provide you with such references.

3. Do you have samples of this kind of work that can be reviewed?

TIP: Reviewing sample deliverables helps set expectations between you and a provider and between you and your internal stakeholders.

4. Can we arrange for personal interviews with the consultants who will be working on this engagement?

TIP: Watch for providers who promise one team of practitioners and then switch to another, often less experienced, crew.

“ In the realm of information security, only two certifications—CISM and CISSP—denote true mastery of the discipline. ”

“ An inability to use fixed pricing suggests a lack of competence and experience. ”

Attribute #3: Value

When it comes to information security, the best value isn't about the lowest price. Rather, it's about getting your organization's money's worth—and enjoying the highest possible levels of flexibility and support. To determine if a provider is offering solid value, ask:

1. Do you offer fixed-price services for routine information security requirements (e.g., vulnerability assessments, web application assessment, policy writing)?

TIP: If a provider is unable or unwilling to use fixed pricing for these types of engagements, it suggests a lack of competence and experience and indicates there may be risk in working with them.

2. Do you stand behind your work with an unconditional commitment to satisfaction based on price offered?

TIP: A satisfaction guarantee removes risk from the buying decision and demonstrates a provider's confidence in its practitioners, methodology, deliverables, and approach.

3. Do you offer flexible agreements, such as retainer services, that allow for changing circumstances and priorities?

TIP: Flexible service agreements demonstrate a provider's trust in you while delivering exceptional value in meeting your requirements as they evolve. (Few things hurt trust more than rigid terms and conditions that simply can't accommodate the realities you're facing!)

Conclusion

Ultimately, your relationship with an information security provider should be a partnership based on trust. That level of collaboration requires that your provider bring to the table intellectual honesty, experience, and value. If you aren't 100% confident that a provider is offering that critical combination of attributes, you should continue looking until you find one that does.

© 2010 Allied InfoSecurity, Inc.

The above material is presented as general information only and does not constitute legal advice or a legal opinion. You should seek the advice of legal counsel with respect to your particular circumstances.

Allied
InfoSecurity

Your security is our business.

1009 West 9th Avenue
King of Prussia, PA 19406
tel: 866.240.0094
email: ask@alliedinfosecurity.com
web: www.alliedinfosecurity.com