THE ULTIMATE GUIDE FOR PURCHASING AN INFORMATION SECURITY RISK ASSESSMENT

Selecting a service provider to perform an information security risk assessment is an important decision. Read this guide and you will discover:

- Why you should be **cautious** of tools that claim to automate a risk assessment.
- 5 **revealing** questions that will help you make the best purchasing decision.
- Big misconceptions that most people have about risk assessments.
- Common mistakes and pitfalls you can avoid when buying an information security risk assessment.

Selecting a service provider to perform an information security risk assessment for your organization is an important decision to make!

Hiring the wrong firm or person to do your risk assessment means that the outcome of the exercise will be disappointing at best. Selecting the wrong service provider could result in :

1. **Wasting Precious Resources** - Time, money and human capital are all precious resources that are finite. The allocation of all three to improve your information security should be completed with the assurance that you achieve the greatest amount of risk reduction. If the risk assessment is performed incorrectly, you will find yourself wasting those precious resources without improving your overall risk profile.
2. **Becoming confused and unclear what to do next** - A risk assessment should produce a clear understanding of the improvements that can be made to better secure and protect the organization from bad actors like computer hackers. Reports and deliverables that contain too much technical jargon tend to be ignored by executives who can allocate resources for cybersecurity improvements.

How can you select the right service provider and avoid these outcomes?

Familiarize yourself with the 5 revealing questions contained in the remainder of this guide. Use them to assess various service providers and you will increase your chances of making the right purchasing decision!!

5 Questions You Should Ask A Cybersecurity Firm Before Hiring Them To Do An Information Security Risk Assessment

Q1: Is a human being completing the risk assessment?

Why ask? Buyer beware - software programs or tools that claim the ability to conduct a risk assessment by scanning your network with little to no human interaction should raise concern! These tools will generally do a nice job discovering vulnerabilities but vulnerabilities are not risks by default. **Risk requires the presence of a vulnerability PLUS the action of threat actor**. To illustrate this concept using an example from the tangible world lets visualize a car. The car is parked and the doors are unlocked. A premature conclusion would be to state that the doors being unlocked translates to risk. If you apply critical thought however, you will discover that the unlocked doors are simply a vulnerability that *could* be exploited. You would need more information to determine actual risk. Is there anything valuable in the car? What is the crime rate associated with the place the car is parked? What would the impact be if someone gained access to the car? The same logic applies to the digital world. A risk assessment requires critical thought to occur beyond the discovery of vulnerabilities by software tools.

Cyberstone's Answer: All risk assessments conducted by Cyberstone are lead by an industry certified and experienced Information Security Consultant. It is there duty to not only consider the presence of vulnerabilities but to also consider the likelihood of threat actors exploiting those vulnerabilities. They provide the reason, logic and critical thinking that software utilities fail to offer.

Q2: Does the assessment provide more than a basic analysis of your cybersecurity control framework?

Why ask? The presence of so many cybersecurity frameworks and standards encourages many service providers to focus solely on the existence of the cybersecurity controls that are prescribed in the framework or standard. The absence or deficiency of any given control does not automatically translate to the establishment of risk.

A risk assessment should involve more than reviewing a checklist of controls, like firewalls or data encryption to determine your unique risk profile. An assessment of your control framework should serve as an input to the risk assessment process but never replace it. If you wanted to buy and apple, you wouldn't shop for a banana. If you want to buy a risk assessment then you should not entertain proposals that only provides a cybersecurity controls assessment.

Cyberstone's Answer: Our risk assessments are performed according to the globally adopted NIST SP800-30 guide for conducting risk assessments. It a comprehensive engagement designed to identify unique risk and threat scenarios vs. simply checking to see if cybersecurity controls are implemented.

Q3:Can they explain how they prepare your organization for the risk assessment?

Why ask? Conducting a risk assessment will require some level of participation from you and your organization. The assessors or consultants responsible for identifying risks and providing recommendations will need input. It is important for them to prepare your organization for the risk assessment so that proper expectations are set and everyone involved clearly understands their roles and responsibilities. Elements of preparation include:

- Understanding the objective and purpose of the risk assessment
- Defining the scope of the risk assessment
- Identifying assumptions of constraints that exist
- Choose the risk model, assessment scales and approach
- Assign roles and responsibilities to all participants

Cyberstone's Answer: We define a custom scope of work for each and every risk assessment and will not start the assessment until all of the proper planning and preparation is completed. It sets the tone for a successful engagement and a fantastic outcome.

Q4: Do they insist on following the NIST SP 800-30 Guide for Conducting Risk Assessments ?

Why ask? The National Institute of Standards and Technology (NIST) is a globally recognized organization that defines standards and best practices. Risk Assessments, according NIST, should be conducted as follows:

- **Identify Threat Sources** - who are the bad actors and what is there capability and intent?
- **Identify Threat Events** - what are the bad things that could occur?
- **Identify Vulnerabilities** - what conditions exist that would influence the success of threat sources?
- **Determine Likelihood** - how likely is it for a threat event to occur?
- **Determine Impact** - what is the adverse impact from threat events occurring?
- **Determine Risk** - what is the actual risk associated with potential threat events?

Neglecting to complete any of these steps reduces your ability to accurately identify risk **and** reduce risk over time. Any attempt to consolidate the exercises listed above is shortsighted.

Cyberstone's Answer: Every risk assessment performed by Cyberstone is strictly aligned with the NIST SP 800-30 guidelines. We never skip a step and understand the value in conducting risk assessments in a way that provides the most comprehensive result.

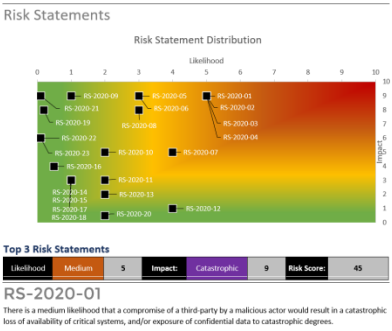
Q5: Do they provide a deliverable that is easy to understand and actionable?

Why ask? The final report, or deliverable provided at the conclusion of the risk assessment should contain all of the content needed for you to:

- Understand your unique risk profile
- Consider formal recommendations to mitigate or reduce risk
- Define information security initiatives & allocate resources
- Satisfy cybersecurity compliance requirements

You should request a sample report or deliverable from the service providers you may be considering to hire. Look for evidence that their report provides the desired benefits listed above. Risk assessment results are documents that should be used to justify the resources required to make big reductions in risk. It is in your best interest for the report to be great, not mediocre or incomplete.

Cyberstone's Answer: Cyberstone risk assessment deliverables are organized, comprehensive and are actionable. We also spend at least and hour with each client to present the deliverable to stakeholders, explain its content and answer any questions. We are happy to share a sample deliverable for you review at any time.



YOUR PURCHASING CHECKLIST!

5 Questions You MUST Ask When Purchasing An Information Security Risk Assessment	Company A	Company B	Cyberstone Secure. Compliant. Assured.
Is a human completing the risk assessment?			✓
Does the risk assessment provide more than a basic analysis of the security controls?			✓
Can they explain how they prepare your organization for the risk assessment?			✓
Do they insist on following the NIST SP 800-30 Guide for Conducting Risk Assessments?			✓
Do they provide a deliverable that is easy to understand and actionable?			✓
Your Choice…			✓