Risk Assessment

DATASHEET

tracesecurity
Practical, worry-free cybersecurity.

877-275-3009 tracesecurity.com sales@tracesecurity

Know Your Risks

Cybersecurity threats are on the rise like never before, and your organization is subject to threats that can impact your IT environment. There are news stories every day on the latest breaches – but how do you keep your organization out of the headlines? The first step is finding out where your risk truly lies. With a risk assessment, you'll get a full view of your organization's risks as well as a recommended action plan on the best way to remediate each vulnerability.

Not Just Identification

During a risk assessment, our experts will identify not only the threats to your assets, but the impact and probability of those threats occurring within your IT environment as well. We evaluate the existence of security controls as well as the effectiveness of the controls used to mitigate threats to your IT security program. We will also identify any residual risk that may still be there after you implement the proper controls to combat threats to your organization. After your engagement, you will have access to our Risk Management platform to streamline your remediation process.

Your Cybersecurity Roadmap

Risk never completely goes away, so it's important to perform regular risk assessments, especially when you have any significant changes to your IT environment. The fact of the matter is that risk is constantly growing, which means your cybersecurity program needs to grow too. Once completing a risk assessment, you'll have a cybersecurity roadmap to help you through your security journey.

A risk assessment is a great way to understand what areas of your IT environment need your attention the most to reduce the overall likelihood of a breach. Once a risk assessment has been completed, you'll understand what controls and procedures you need to implement as well as other IT-related areas that may need additional testing. Don't waste your time and resources on solutions you don't really need – use the results from your risk assessment to truly know what areas need your attention so you can make the most of your budget.

After a Risk Assessment You Will:

- **Understand your security posture and risk level present**
- **Have a recommended action plan for remediation**
- **Have a starting place for your cybersecurity roadmap**

Frequently Asked Questions

What is the difference between a risk assessment and an IT audit?
A risk assessment reports the resulting residual risk after evaluation of threats to your assets and current mitigating controls, whereas an audit proves/tests that you have implemented the prescribed and asserted controls.

What is included in "IT security?"
Information technology is one element of your information systems, but there are usually physical, technical, procedural, and personnel-related elements too. Combined, these encompass your Information Security program, which includes IT Security.

How much disruption will this cause in my day to day operations?
Aside from interviews with key stakeholders, this service causes little to no disruptions in normal business activities.

What kind of physical access do you need?
No type of physical access is necessary. We can perform risk assessments remotely or onsite depending upon your preference.

How many times should I get a risk assessment and how often?
Risk assessments should be done upon major changes to the processes or information systems, or at least once per year.

Who do you need to talk to in my organization?
Any stakeholder with knowledge of the technical, procedural, personnel, and physical controls employed by the organization to protect information.

Are you going to look at my policies?
A policy document may be reviewed at the client's request in order to gain insight into any particular policy, process or control.