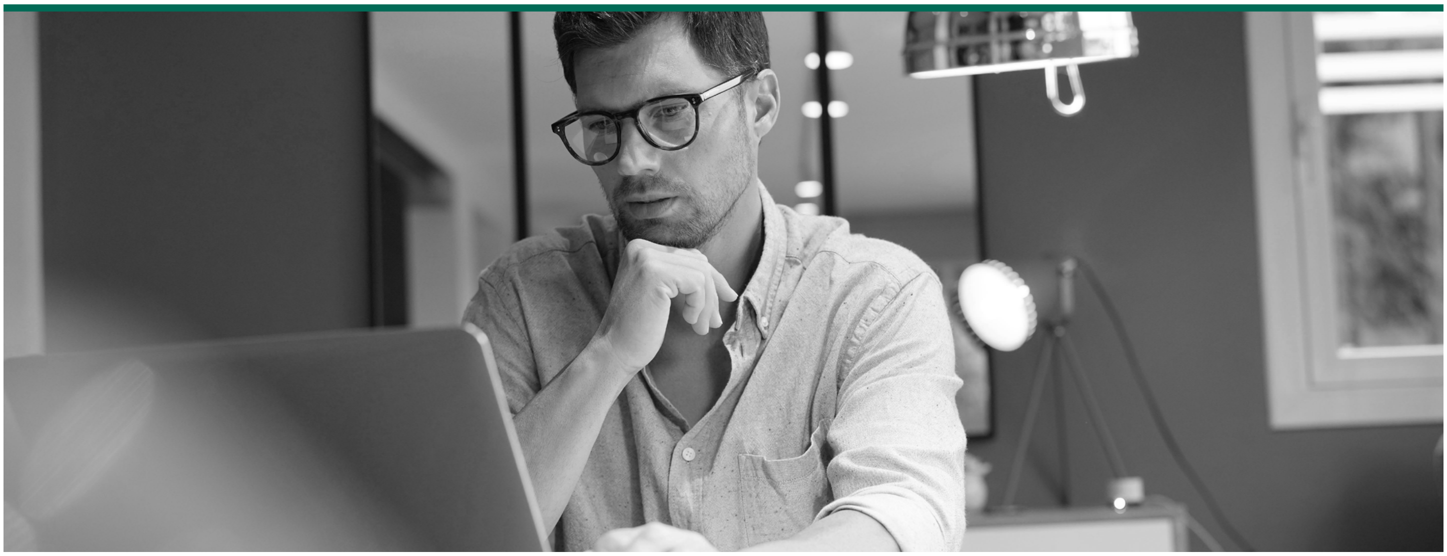
FORTRA™

GUIDE (CORE SECURITY)

What to Look for in a Pen Test Report



Nowhere is a good pen test report more important than in a company facing strict compliance regulations. Nowadays, that means all of them. In many ways, there are more stakeholders looking in on pen test reports - and more riding on them – than ever before. Here's what to look for in a good one.

Why Strong Pen Test Reports Are Critical

Not all pen test reports are created equally. If you are in finance, you need a report that caters to SOX or PCI DSS. In healthcare, one that takes HIPAA obligations into account. And no matter what industry you are in, the audience for your pen test report will always be bigger than your immediate security circle; many times, your board, compliance auditors, and even customers will be looking at the results, and that can determine your ability to do business with them down the road. If you are in a SOC 2-based company, your partners will want evidence that pen tests have been done, and this all circles back to the humble pen test report. So, for this reason the report is your friend. Deliver a poorly written report, and you could have problems.

How Pen Test Planning Influences Pen Test Reports

A report is the final product of the pen testing exercise. Consequently, the pen test report will only be as good as the pen test itself. One of the most critical parts of a pen test occurs right at the start when the pen testing team meet with stakeholders to clearly outline goals, expectations, and limitations. Before the test begins, stakeholders and testers should have the following items well-defined and agreed upon:

- **SOW (Statement of Work)** | This states a high-level overview of the work to be completed. It also, unfortunately, needs to include a limitation of liability clause to cover any legal bases. For example, delineating that a "test" reflects the results at a point in time, not approval of Y Corporation's overall security, etc.
- **Detailed Scope** | What is included in the pen test? What specific systems and applications will be tested? Which security controls need to be evaluated? What data are testers allowed to access? Who in the company will know that the test is occurring? Details matter here.

- **Exclusions** | What is NOT to be tested? While testing the entire environment would be great, it's simply not realistic. Testers need to have a narrowed scope to go beyond surface level and target their efforts to more thoroughly examine specific, business critical assets.
- **Methodology** | How the test will be performed. "Methodology" is very different from "scope," but tightly entwined. This provides a general picture of what threat tactics are to be used, including social engineering ploys, Man-in-the-middle attacks, injection attacks, and more.
- **Timeframe** | The "when," or how long testers have and over what period of time.

Defining a well-scoped pen test ensures that everyone is on the same page and also guarantees a pen test report will contain data about parts of the infrastructure that are of the greatest concern to the organization. Additionally, the quality of the pen testing plan documentation is a good indicator of the experience and capabilities of the testing team, as a seasoned team will more likely produce a quality final report.

Anatomy of a Pen Test Report

Test reports should be brief and concise, but we must also remember to provide detailed appendices of supporting documentation outside the report for those who want and are "allowed" to dig into the findings. Vendors need to bear in mind that regulators, their client's clients, and others will be asking for these. That's why it's best to only cover the facts in the report and avoid conjecture. Along those lines, here are the layout requirements widely regarded to be essential in any enterprise-level pen test report.

Methodology and Scope | The "top end" of the test report should specify the overall procedure of the test, essentially providing a recap of everything that was laid out in the initial plan. This ensures that anyone who wasn't present during that process can still understand the parameters of the test.

Results | The body, or the "meat and potatoes" of the report, is the summary of the results. Types of findings can be laid out in various ways, but generally are laid out based on severity of findings. Depending on the security frameworks followed by the client (such as NIST, MITRE, COBIT, and more), you may want the findings to be presented in a way they can be brought into other risk management programs. Be open with your team/vendor about this and remember to ask for sample reports upfront in the planning stages.

Recommended Actions | The recommended actions are examples of potential mitigating controls in the form of a high-level guide, not a step-by-step list of how to fix everything.

Summary | The summary states the boiled-down facts and is arguably the most important part of the report. This is where the business case is often made, as non-technical executives search here first (and sometimes, only) to view the results of their investment and trust in you as a pen test vendor. If you have a sloppy, hard-to-read summary, you won't be rehired. While the layout is very dependent on the engagement type, here are some universal tips for a winning summary:

- **Prioritize Critical, High, and Medium** severity findings, while briefly reviewing the Low or Informational ones with a simple statement like "X Low and Y Informational findings were discovered."
- **Include practical infographics** like charts and graphs and avoid fluff data.
- **Provide fact, not opinion**, and avoid using words like "numerous," "systemic," and "ongoing" for that reason (no matter how well-informed your opinion might be).
- **Classify the risks** does a finding effect an organisations valuable reputation, increase the potential for a breach, data loss, or legal action? The report can help stakeholders understand the consequences of mitigating, accepting, or transferring the risk.

Keep in mind that what stakeholders are looking for today is the business impact of found vulnerabilities in the system. If they can't trace potential weaknesses to breaches and dollars, the report isn't doing its job. Make sure that the stakes are clear and that the threats are clearly defined. Also, a vendor that knows your environment and has been with you for multiple engagements could instinctively know which systems matter the most and what matters to your business and will be better able to align with those goals without additional time and training. It's worth noting that there is also a bit of a notion that a vendor that has been with you "too long" may be seen as being able to become complacent in their testing and start to give less effort. For this reason, some organizations limit the duration of a contract to three to four years. However, it is all about weighing the benefits. If your vendor is doing a wonderful job, has dynamic testers, and is evolving with you, a switch may be unnecessary. If not, it may be worth it to take the time to interview new vendors.

Fortra's Pen Testing Solutions

Basic third-party pen testers will do little more than deliver the default report generated by their analysis tools. However, Fortra's penetration testing services deliver unique reports that incorporate threat data and show trends in vulnerability distribution. This allows companies to see which services are the weakest and shore up defenses strategically, getting the most protection per security dollar spent.

Composed of experienced cybersecurity professionals, Fortra's security services are a safe and secure outside opinion that provide a fresh perspective on the state of your security. They begin with a collaborative planning process to provide engagements tailored to your specific needs and environment. Upon completion of an engagement, organizations are given robust reports that help meet compliance requirements and provide new insights to bolster your security.

Additionally, by using Fortra's automated pen testing tool, Core Impact, organizations can put their internal resources to use and leverage even inexperienced individuals to test against network, client-side, and web applications. By having a centralized solution that carefully logs data and tracks the penetration process, organizations will have the data they need to generate detailed reports all in one place. Having your own internal testing process to uncover threats allows you to turn risk management into a proactive, routine strategy. This makes third-party testing less of a fire drill, and more of a validation of your efforts.

Putting Your Best Foot Forward

In a world where security is starting to become the currency of business, how you present your security posture matters. The quality of the pen test report you deliver to your stakeholders will largely determine the kind of relationship you have with them going forward, whether that be a business partnership or a compliance audit passed. The better, clearer, and more thorough your report – and the more advanced the tests on today's modern services – the more confidence it will build in your organization's overall viability going forward.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.