turingpoint.

GUIDE

How to Choose the Right Pentest Provider

August 20, 2026 - Version 2.0

Created by:
turingpoint GmbH

turingpoint GmbH
Neuer Wall 80
20354 Hamburg
Germany

Phone: +49 40 52477883
Email: hello@turingpoint.de
Web: turingpoint.de

Commercial register: 157676
VAT ID: DE325011218

turingpoint.

Table of Contents

Introduction

Finding the right provider for penetration testing can be a difficult process, especially for anyone who does not deal with IT security every day. What do I actually need? How do I recognize genuine technical expertise? How do I spot unqualified providers? And what does solid documentation look like, the kind that holds up before regulators and auditors?

In this guide we present **seven questions** you should ask every potential provider for your next pentest. Afterwards you will know what matters in the selection, how to compare proposals, and how to make the best choice for your requirements, all without your own security department.

For every question we also show transparently **how turingpoint answers it**. That way you can use our qualifications directly as a benchmark for your comparison.

> **turingpoint at a Glance**
>
> **BSI-certified** IT security provider. Certified **ISMS to ISO 27001**. More than **200 completed projects**. In-house vulnerability research with **over 50 published CVE advisories**. Experience as a **red team** (DORA, TIBER-EU, NIS-2).

What Matters Most: Reputation

A provider's reputation for high quality and trustworthiness is one of the most important aspects. Before the first conversation, look into their background and expertise: what do you find when you research the provider? Are there in-depth technical articles, original research, or blog posts that match your technical requirements? A strong professional footprint is a reliable signal of real competence and is hard to fake.

01

How Automated Is the Pentest?

TECHNICAL EXPERTISE

Why does this matter? Automated tools and scanners are the starting point of every pentest, but they routinely miss the larger, business-critical risks. The share of manual testing is therefore a simple indicator of a provider's quality.

A high-quality pentest is predominantly a manual, in-depth process. Around **90 percent of the work should be manual**. If a provider states that the test is largely automated, or asks few questions about your environment, be cautious: such assessments create a false sense of security and bring additional risks with them.

The experience of the pentester has a greater influence on the result than the tools used. Scanners contribute only a little to a thorough test.

> **How turingpoint Works**
>
> Our pentests are manual, structured, and attack-oriented, carried out by experienced analysts who also simulate real attackers as **red teamers**. We use automated scans deliberately to cover breadth; depth comes from manual analysis.

02

Which Standards and Methods Are Used for Testing?

EFFECTIVE PROCESS

Why does this matter? Every pentest needs a clearly defined methodology and a structured process. This establishes a traceable workflow, minimizes misunderstandings, and maximizes both the security value and the significance of the results.

The established standards and methods include:

- **OWASP Testing Guide / OWASP Top 10** for web, API, and mobile applications (industry standard)
- **OSSTMM, NIST SP 800-115, PTES, ISSAF** for infrastructure pentests
- **BSI guideline for penetration testing**, required for compliance with the German IT-Grundschutz standards
- **PCI DSS** as the minimum standard for the security of payment systems
- **MITRE ATT&CK** as a framework for realistic attack simulations and red teaming

Make sure the provider uses a clearly documented, industry-standard methodology, and that every test begins with a proper reconnaissance and information-gathering phase. This is an often-neglected but decisive detail.

How turingpoint Works

We test along **all established methods** (OWASP, OSSTMM, NIST, PTES, ISSAF, the BSI guideline, PCI DSS, and MITRE ATT&CK) and cover the full spectrum: web and API pentests, mobile apps, internal and external infrastructure, and cloud environments in **AWS, Azure, and Google Cloud**. As a **BSI-certified** provider, our tests are Grundschutz-aligned and regulatory-compliant.

03

What Does the Documentation Process Look Like?

DOCUMENTATION

Why does this matter? The report is the actual result of a pentest: it is where you understand where your risks and weaknesses lie, and it often goes to people who never spoke with the provider. Clear, thorough documentation is therefore decisive, and it must address both technical experts and management at the same time.

Ask every provider for a **sample report**. Good providers keep samples ready for every type of pentest they offer. A solid report always contains:

- **Management summary:** a non-technical overview of the engagement for leadership
- **Vulnerability overview:** prioritized by criticality (for example CVSS)
- **Detailed findings:** with proof of concept, evidence, and reproducibility
- **Concrete remediation recommendations:** actionable for your teams
- **Traceable assessment:** methodology, scope, and testing depth laid out transparently

How turingpoint Works

Our reports combine an understandable management summary with technically solid findings, including proof of concept and prioritized remediation recommendations. On request we provide a **free sample report** in advance.

04

Are Free Retests Included?

SCOPE & IMPACT

Why does this matter? A pentest should not only assess security but improve it. Whether your countermeasures have the desired effect only becomes clear in a subsequent validation. During the retest, all identified vulnerabilities are checked again and the result is incorporated into an updated final report. You can also present this evidence to external stakeholders.

A retest is an important part of a pentest. A good provider does **not charge extra** for it. Anyone who cleanly documents identified vulnerabilities with proofs of concept has only minimal additional effort during the retest. Leading providers therefore offer it free of charge.

> **How turingpoint Works**
>
> Re-checking remediated vulnerabilities is a fixed, **free** part of our pentest. You receive an updated report that documents the successful remediation.

05

Is There Security Engineering Expertise?

TECHNICAL EXPERTISE

Why does this matter? Vulnerabilities that are found must be fixed. Security engineering forms the bridge between software development and IT security: experienced security engineers support you in fast-moving development work with remediation, and already during development with the secure implementation of critical code sections.

Make sure your provider not only **identifies** vulnerabilities but can also support you with their **remediation**. If you lack your own security department, this access to experienced consultants is especially valuable.

How turingpoint Works

As a boutique consultancy, we combine offensive security (pentest, red teaming) with well-founded security engineering and security architecture. The fact that we publish our own **CVE advisories** and research zero-days feeds directly into solid, practical remediation recommendations.

06

Are Continuous Security Processes Offered?

SUSTAINABILITY

Why does this matter? In modern development environments (DevOps, CI/CD), security processes should not be occasional but firmly anchored. A pentest is a snapshot and, with short-lived software artifacts, quickly outdated. Automated security in the pipeline does not replace a full pentest, but it keeps the security level high over time.

For this reason, ask about expertise in automated and continuous security even for manual pentests. This ensures a long-term collaboration and lets you check whether the provider is up to date and suitable for future DevSecOps projects.

How turingpoint Works

We integrate security permanently into your development and operations processes through DevOps security and security architecture, from static code analysis to secure cloud transformation. As the operator of a **certified ISMS to ISO 27001**, we know how to anchor security in a process-driven, audit-proof way.

07

How Are AI Systems Handled?

FUTURE-READINESS

Why does this matter? AI systems such as large language models (LLMs), RAG applications, and autonomous AI agents create entirely new attack surfaces that classic pentests do not cover: prompt injection, leakage of confidential data through the model, insecure connection of tools and functions to AI agents, and manipulated training and knowledge sources. Anyone integrating AI into products or processes needs a provider who understands these risks and tests for them specifically.

Make sure your provider can do two things: first, **secure and test AI systems**, guided by established references such as the OWASP Top 10 for LLM applications (prompt injection, RAG security, hardening of agents and their tool access). Second, they should command **AI-supported attack and analysis methods** and use them sensibly in assessments, without replacing the depth of manual work.

How turingpoint Works

With our **AI in Cybersecurity** practice, we test and harden AI systems, from LLM applications and RAG architectures to autonomous agents, along the OWASP Top 10 for LLMs. At the same time, we use AI deliberately in our assessments to increase breadth and efficiency, while the security-critical analysis stays in experienced hands.

Why turingpoint

The seven questions guide you safely through the selection. In summary, turingpoint answers them like this:

Our Qualifications at a Glance

- **BSI-certified IT security provider:** Grundschutz-aligned and regulatory-compliant penetration tests
- **Certified ISMS to ISO 27001:** security anchored in an audit-proof, process-driven way
- **Over 50 published CVE advisories:** in-house vulnerability research with root-cause analyses and proofs of concept
- **All established testing methods:** OWASP, OSSTMM, NIST, PTES, ISSAF, the BSI guideline, PCI DSS, MITRE ATT&CK
- **Experience as a red team:** realistic attack simulations under DORA (Art. 26/27), TIBER-EU, and NIS-2 (Art. 21)
- **AI security:** securing and testing LLM applications, RAG, and AI agents (AI in Cybersecurity)
- **Over 200 completed projects:** for clients from startups to large enterprises
- **Free retests:** as a fixed part of every pentest

Original Research, Not Just Tool Operation

Unlike pure scanner operators, turingpoint conducts its **own vulnerability research**. Our team identifies, verifies, and reports zero-day vulnerabilities in widely used software and publishes them as security advisories with **CVE IDs**, root-cause analyses, and proofs of concept. This offensive depth feeds directly into your pentests. You benefit from first-hand attacker knowledge.

Full Testing Spectrum

Web and API applications, mobile apps, internal and external infrastructure, cloud environments in AWS, Azure, and Google Cloud, as well as complete **red team assessments** and the hardening of AI systems, backed by an industry-standard methodology and regulatory compliance.

About Us

turingpoint is a boutique consultancy founded by security experts with a focus on cyber security. Our experienced security experts help you protect your applications and systems and implement progressive security concepts. In IT security in particular, we stand out through fresh ideas, creativity, and careful work, with offices in Hamburg (headquarters), Paderborn, and Zurich.

The search for a penetration testing provider can be challenging. The seven questions in this guide lead you safely through the process. Trust, technical expertise, the quality of the staff, and the depth of the reporting are among the most important selection criteria. In addition, consider pricing structure, references, and industry experience, and formulate your own questions until you feel confident about your provider.

Contact

Email: hello@turingpoint.de **Phone:** +49 (0)40 52477883 **Web:** turingpoint.de

Arrange a no-obligation initial conversation. We are happy to advise you on your next pentest.