CISO GLOBAL

A **CISO GLOBAL** WHITE PAPER

How to Get a Boardroom-Ready & Audit-Ready Penetration Test

Table of Contents

What Is A BR/AR Penetration Test?

Choosing the right penetration testing provider can be critical to the success of a security program.

Imagine spending thousands of dollars on a PCI penetration test, only to find out, come audit time, that the penetration test does not meet PCI requirements. IT organizations with an inadequate PCI penetration test can be hit with fines, findings of non-compliance, and even higher liability burdens. The IT leaders are often the ones left holding the bag when the penetration test does not live up to its promise.

Imagine getting a penetration test report that is lengthy or overly technical and has to be interpreted for your board or executive management body. When IT leaders don't fully understand the penetration test report, executive leaders can come away with misunderstanding and a false sense of security. An executive body that lacks understanding of the security program will have unrealistic expectations placed on IT leaders and will lead to a security program that is reactive in nature.

Instead, what if we were to tell you that there are three simple steps to follow in the penetration testing process to ensure your penetration test will be boardroom-ready and audit-ready (BR/ AR)?

What does this really mean?

A BR/AR penetration test report will meet these two criteria:

1. It will meet your compliance requirements (e.g. HIPAA, PCI, NERC CIP, FFIEC) for technical testing.
2. It will be easily interpreted by executive management.

Simple, right?

It might surprise you that most penetration test providers do not deliver a BR/AR penetration test. For over a decade we have built highly-effective security programs, and we have seen very poor penetration test reports that fail completely or only meet one of the two criteria.

It takes a company that is truly invested in your long-term success with a proven track record of building highly effective security programs to deliver a BR/AR penetration test. In this white paper, we will show you the step-by-step process to ensure your next penetration test is boardroom-ready and audit-ready (BR/AR). As a bonus, at the end of this white paper, we have compiled a penetration testing buyer's checklist that will help you identify the best penetration test provider.

Step #1: Does the Penetration Test Provider Understand Your Compliance Requirements?

A quality penetration test provider will understand how a penetration test will help you meet compliance requirements. A simple test of the vendor can quickly help you ascertain companies who do not understand your specific compliance needs.

PCI DSS

If you are required by the PCI DSS to perform penetration testing, ask the penetration test provider one of the following Red Flag questions.

Question #1: "To meet requirement 11.3.2 of the PCI DSS, can we conduct the internal penetration test from inside the perimeter of the card holder data environment (CDE)?"

Red Flag Answer: Yes

Correct Answer: To meet requirement 11.3.2, you must perform the internal penetration test from the perspective of an out-of-scope LAN segment that has access to the CDE perimeter. A penetration test performed within the CDE cannot be used to meet requirement 11.3.2.

Question #2: "If we have an antivirus management server outside the CDE that manages antivirus agents installed on systems inside the CDE, does the antivirus server need to be included in the internal penetration test scope?"

Red Flag Answer: No

Correct Answer: Critical systems or those systems that may impact the security of the CDE should be included in the scope of the penetration test. The antivirus management server has the ability to affect the security of systems inside the CDE, so it should be considered a "critical system" and should be included in scope.

HIPAA

If you have HIPAA compliance requirements, ask the penetration test provider one of the following Red Flag questions,

Question #1: "Does a penetration test help meet HIPAA compliance requirements?"

Red Flag Answer: Penetration testing does not support HIPAA compliance.

Correct Answer: Penetration testing can help meet the Technical Evaluation requirement of HIPAA implementation specification §164.308(a)(8).

Question #2: "In order to support the Technical Evaluation requirement of HIPAA (§164.308(a)(8)), does it matter what the scope of the penetration test is?"

Red Flag Answer: No

Correct Answer: To support the Technical Evaluation requirement of HIPAA, the scope of your penetration test must include assets that can store, receive, maintain, or transmit electronic protected health information. For instance, a PCI penetration test that does not include any HIPAA-related assets cannot be used to support the Technical Evaluation requirement.

Other Compliance Requirements

Question #1: "Does a penetration test help meet X compliance requirements?" Where X is your specific compliance requirement.

Red Flag Answer: Penetration testing does not support X compliance.

Correct Answer: Penetration testing usually supports compliance requirements even if not specifically required. If you are curious about your specific compliance environment, please contact CISO Global to discuss.

Step #2: Can the Penetration Test Provider Deliver a Boardroom-Ready Report?

It is important that the results of a penetration test be easily understood by executive management and the board. If you need a CISSP to understand the report, it will be of little value to executive management. If you translate the report, you run the risk of misrepresenting the facts and the burden is placed on your shoulders. Instead, a penetration test provider should deliver results that are easily understood by executive management bodies.

Even if your current executive management body is not in the loop on security, having a boardroom-ready report will be extremely helpful when they are brought into the loop. More and more boards are becoming involved in security oversight. You will want to prepare yourself for this shift if it hasn't yet occurred at your company.

A boardroom-ready penetration test report will contain an executive summary that gives a high-level summary of the engagement and overall risk of each engagement component.

The report itself will have a risk/severity score assigned to each finding so that remediation actions can be prioritized.

To evaluate a penetration test provider's reporting, first request a sample report. Here are some Red Flags to look out for:

1. The penetration test provider is unable/unwilling to provide a sample report.

2. Identified findings do not have an assigned risk/severity score.

3. The sample report does not contain an executive summary with an overall risk rating and detailed definitions for the risk levels.

4. The report does not contain a testing narrative and methodology.

5. The executive summary is not easily understood by a non-technical audience.

6. The penetration test provider does not offer an executive presentation at the conclusion of the engagement.

Step #3: Does the Penetration Test Provider Include Remediation Validation?

Many penetration test providers simply conclude the engagement upon delivery of the final report. What if their recommendations are not clear? What if the IT provider attempts to correct the vulnerability, but opens up another vulnerability in the process? The IT provider may not identify these issues until the next penetration test, leaving the organization exposed to additional risk.

Look for a penetration test provider that includes remediation validation after report delivery. This will allow IT providers to validate that remediation activities were successful. Ensure the penetration test provider will update the report to reflect the new risk profile. This will give you documented third-party evidence that remediation was successful, simplifying your paperwork.

A post-remediation report will provide a higher-level of assurance to auditors and your executive management and it will also demonstrate that the IT organization is doing its due diligence to promptly correct identified vulnerabilities.

Penetration Test Buyer's Checklist

Does the vendor...	Vendor A	Vendor B	CISO GLOBAL
Understand your compliance requirements (Step #1)?			✓
Deliver a boardroom-ready report?			✓
Offer remediation validation after report submission and issue a post-remediation report to reflect updated risk profile (Step #3)?			✓
Provide a sample report?			✓
Include an executive summary in their report with an overall risk ranking for each engagement component?			✓
Assign a risk rating for each identified vulnerability?			✓
Include a testing narrative and methodology in the report?			✓
Deliver reports with highly actionable recommendations?			✓
Have a proven track record for building highly effective security programs?			✓
Present findings to executive and management bodies?			✓
Have expertise in web application penetration testing?			✓
Conduct manual testing & not solely rely on automated scans?			✓
Conduct testing remotely to minimize your burden?			✓
Ensure all false positives are removed from the report?			✓
Offer penetration testing as a component of a risk assessment?			✓
Offer targeted attack simulation (e.g. phishing emails or phone calls used in conjunction with the penetration test)?			✓
Offer client references from similar companies?			✓

About CISO Global

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, security engineers, and around-the-clock analysts.

To learn more, visit www.ciso.inc.

AICPA SOC
aicpa.org/soc4so
SOC 2® Type II Audited