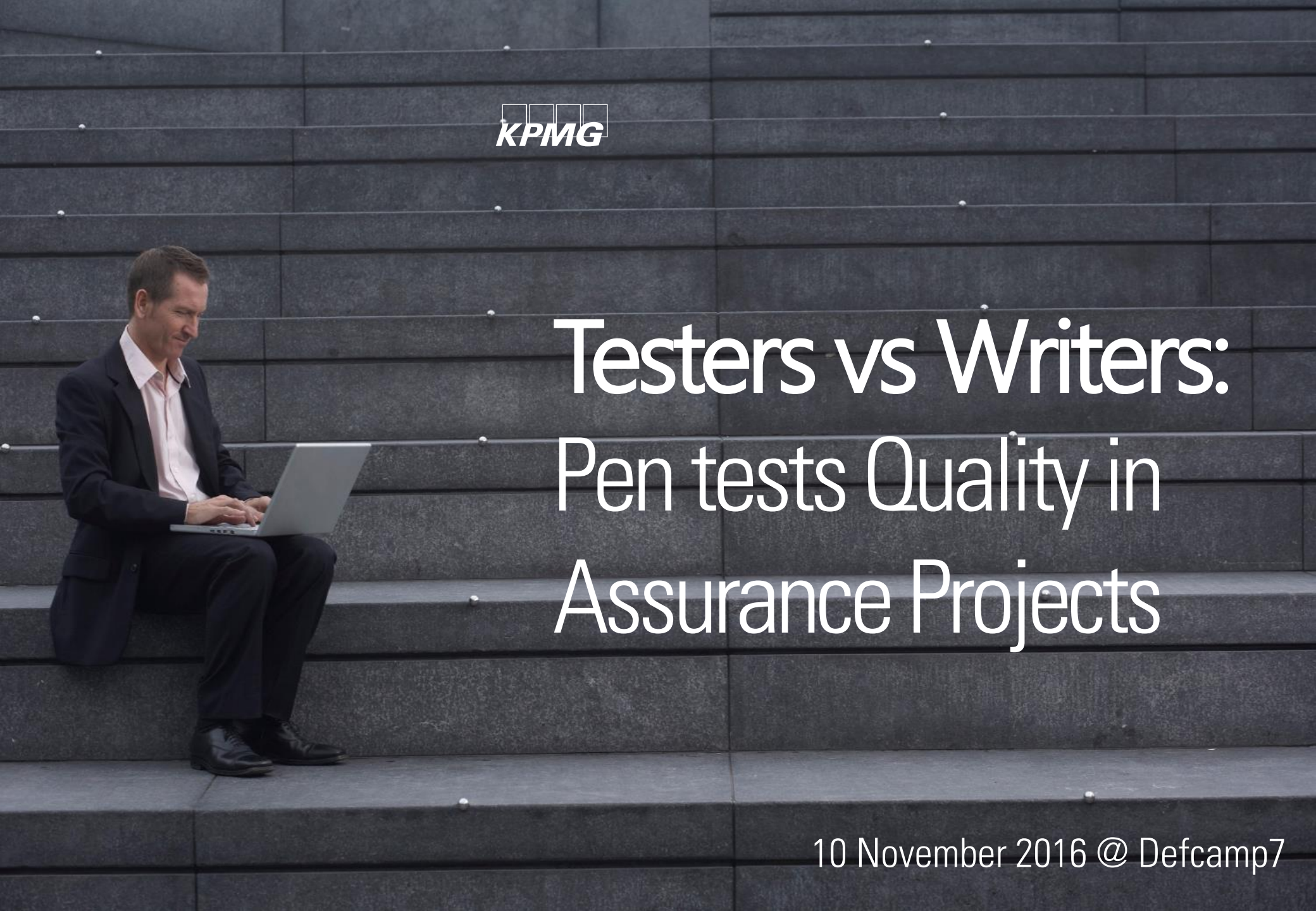


KPMG

Testers vs Writers: Pen tests Quality in Assurance Projects

10 November 2016 @ Defcamp7

Contents

INTRODUCTION

Gabriel Mihai Tanase

Director, IT Advisory
Cyber Security Services
KPMG in ROMANIA

Short background:

- More than 14 years in KPMG
- IS auditing background
- Set-up the Pen Test team in KPMG RO in 2003

CONTEXT

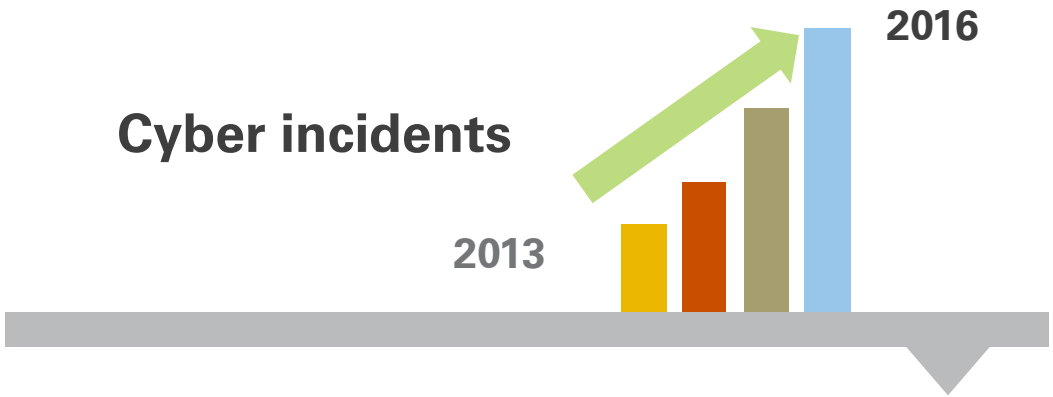
New/ updated regulation requesting periodic IS audit and penetration testing

IS auditor to verify and describe how pen test was performed

Making Information Security key to business

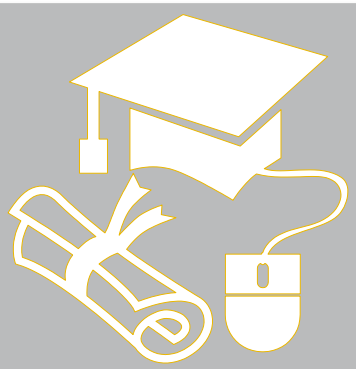
IT Risk vs Operational Risks

Evolved approach based on risk level



AUDITORS AND PEN TESTERS

IT Auditors Register



More than 20 auditors already accredited:

- **Audit companies**
- **Individual auditors ??**

WHAT ABOUT IS AUDITING STANDARDS

IS AUDIT and ASSURANCE STANDARD – 1206 USING THE WORK OF OTHER EXPERTS

Defines 7 statements regarding the auditor responsibilities when considering the use of work of other experts.

IS AUDIT and ASSURANCE GUIDELINE – 2206 USING THE WORK OF OTHER EXPERTS

Provides guidance to IS audit and assurance professionals when considering the use of work of other experts.

STANDARD STATEMENTS

1206.1: consider using the work of other experts

1206.2: assess and approve the adequacy of the other experts' professional qualifications, competencies, relevant experience, resources, independence and quality-control processes prior to the engagement.

1206.3: review and evaluate the work of other experts as part of the engagement, and document the conclusion on the extent of use and reliance on their work.

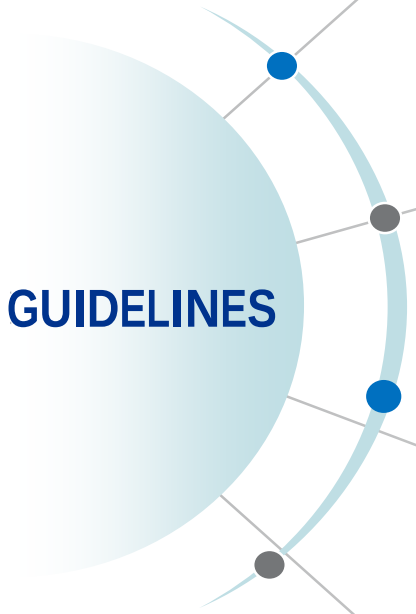
1206.4: determine whether the work of other experts, who are not part of the engagement team, is adequate and complete to conclude on the current engagement objectives, and clearly document the conclusion.

1206.5: determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report.

1206.6: apply additional test procedures to gain sufficient and appropriate evidence in circumstances where the work of other experts does not provide sufficient and appropriate evidence.

1206.7: provide an appropriate audit opinion or conclusion and include any scope limitation where required evidence is not obtained through additional test procedures.

GUIDELINES



SECTION 2.2: Assessing the Adequacy of Other Experts

- independence and objectivity of the other experts
- professional qualifications, competencies and relevant experience
- use of quality control processes

SECTION 2.4: Evaluating the Work of Other Experts Who Are Not Part of the Audit Engagement Team

- cautious in providing an opinion on cases when do not have access to relevant supporting documentation and work papers
- assess the usefulness and appropriateness of reports issued by the other experts
- responsibility to determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report.

WHAT ABOUT INDEPENDENCE

AUDITOR HAS TO BE INDEPENDENT IN RELATION TO THE COMPANY AND THE IS AUDITED

The auditor has to be capable to prove the independence requirements.

IS auditing standards address:

- **Organizational Independence**
- **Professional Independence**

Performing pen test as part of the audit (e.g. as technical audit procedures) is breaching the independence? – in scenarios without any implication in addressing the findings.

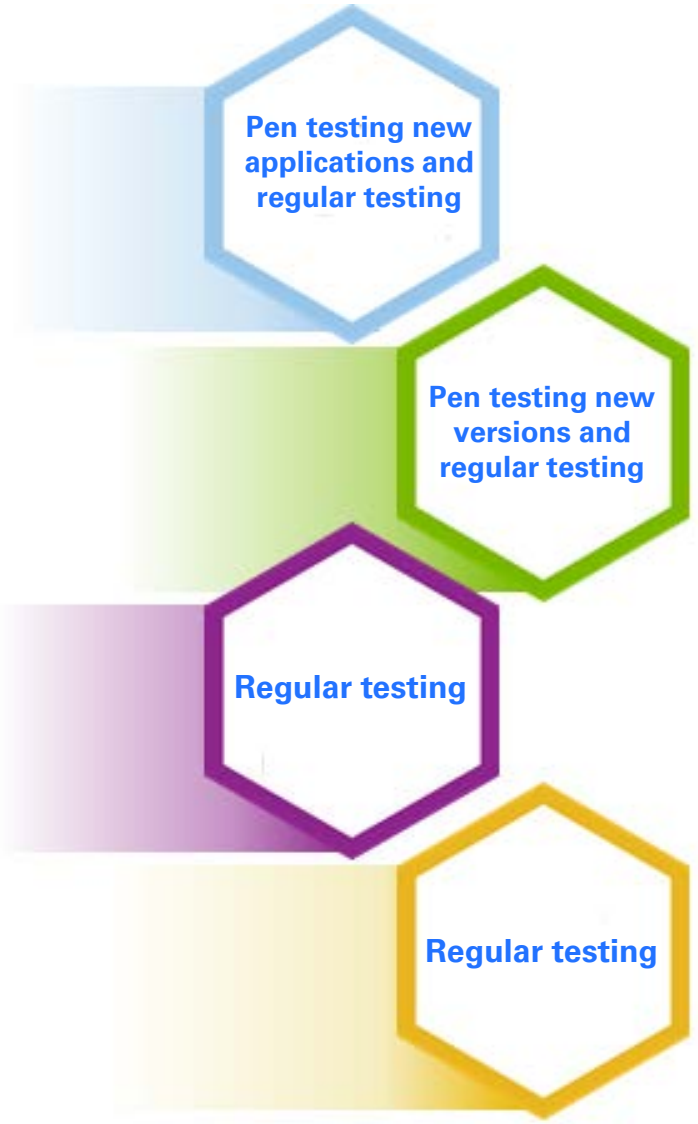
Can be penetration testing associated to consulting services in such a scenario?

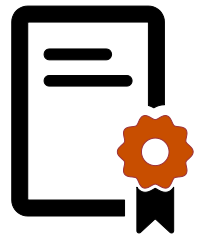
PEN TEST: BETWEEN REGULATORY AND CYBER MATURITY

Pen test for the first time due to regulatory requirements

Report with low number of vulnerabilities, most of them low risk rating

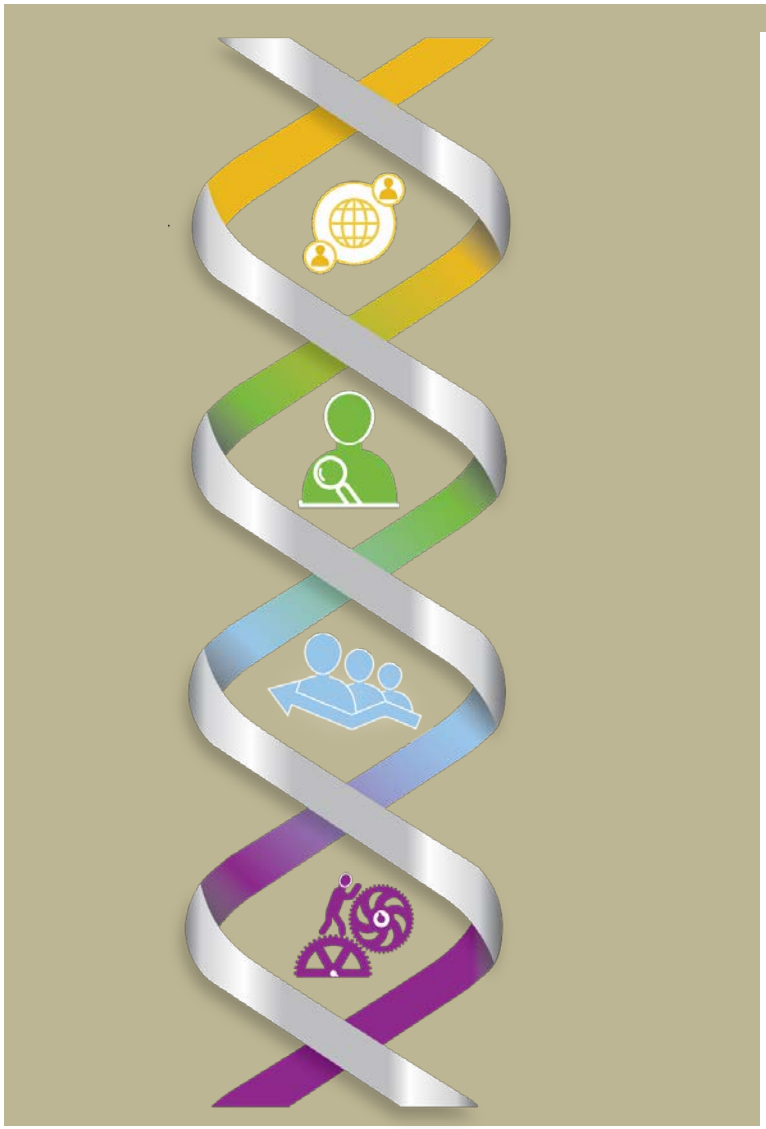
Good pen tester or good report writer?





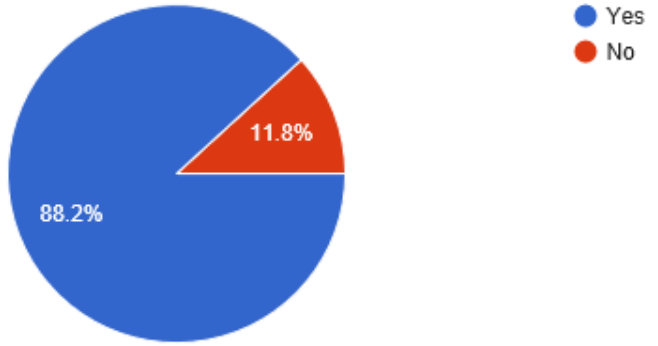
Cyber Maturity

OUR SURVEY

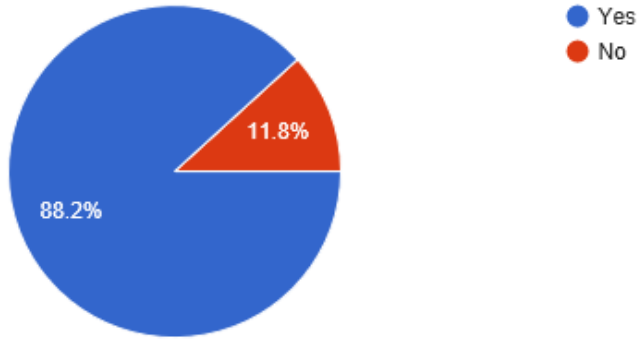


Short survey on vulnerability assessment and pen test

Did you performed vulnerability assessments in the last 12 months?

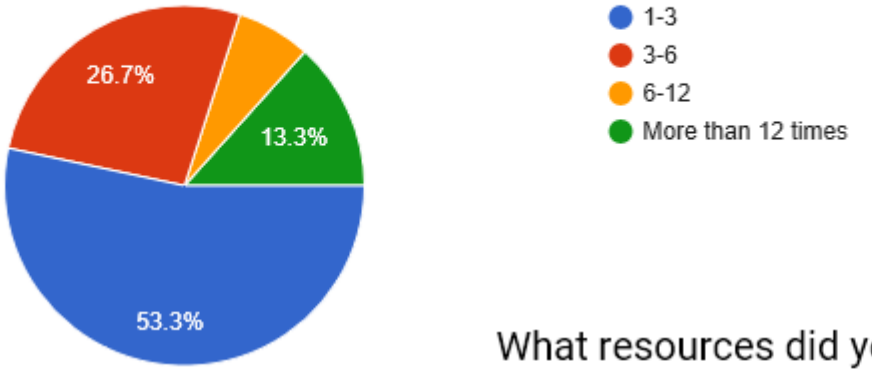


Did you performed penetration testing in the last 12 months?

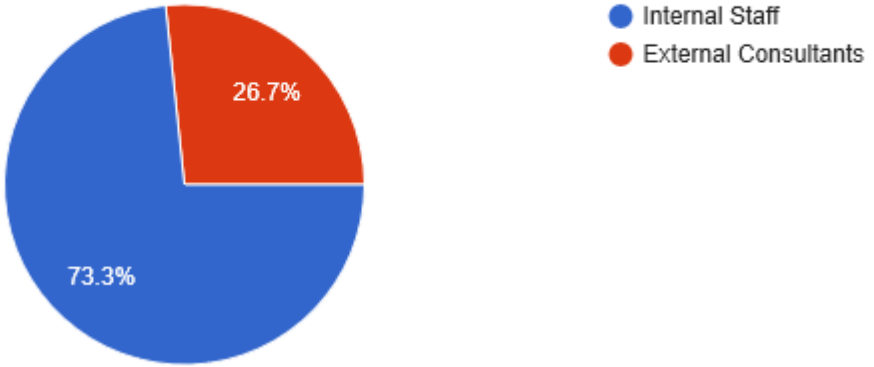


VULNERABILITY ASSESSMENT

How many times?

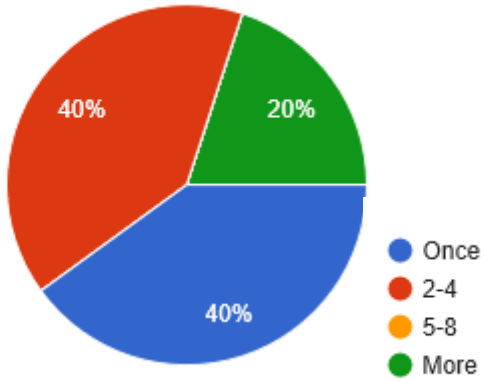


What resources did you used?

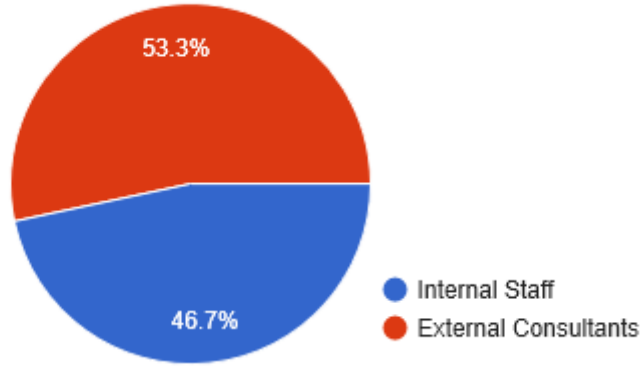


PENETRATION TESTING

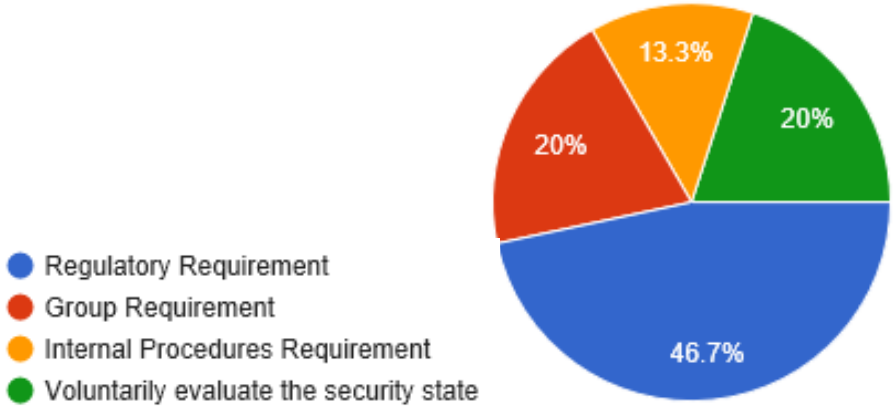
How many times?



What resources did you used?

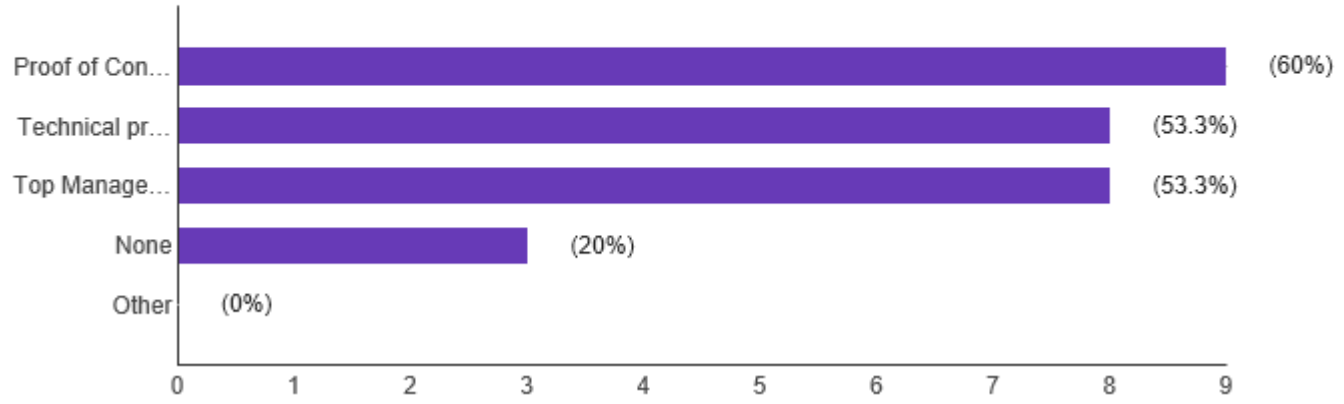


Why did you performed penetration testing?

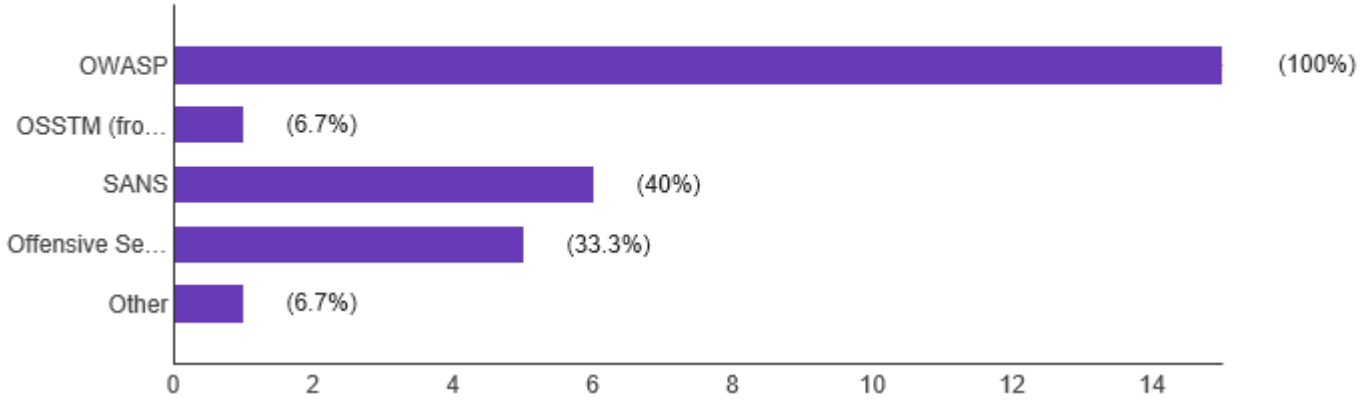


PENETRATION TESTING

What was the deliverable of the penetration testing project in addition to the report?

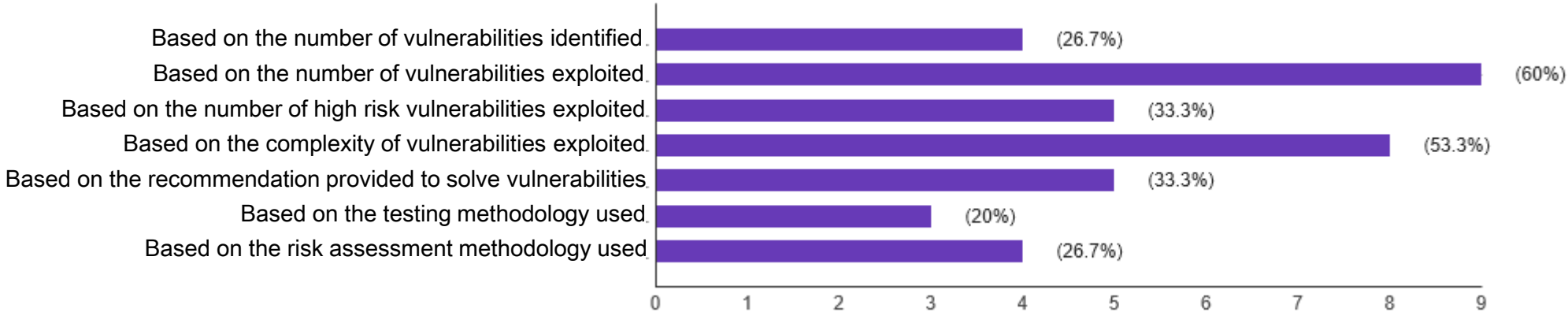


What was the methodology used by the penetration tester?

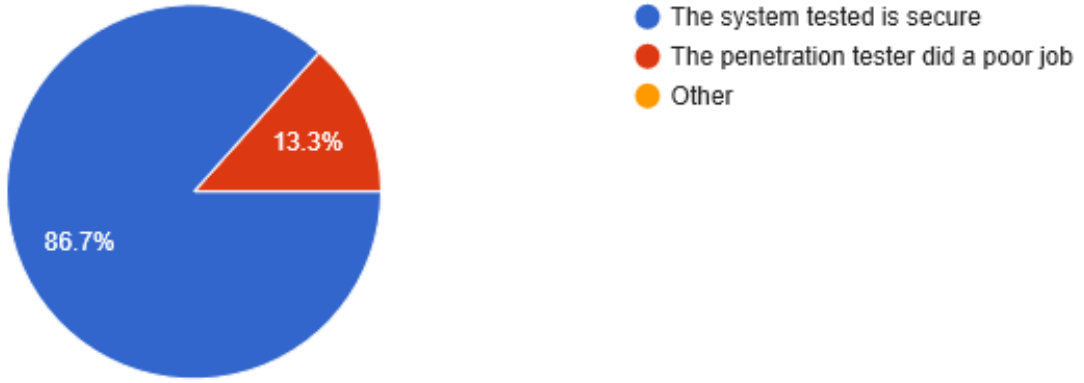


PENETRATION TESTING

How do you evaluate the penetration testing report?

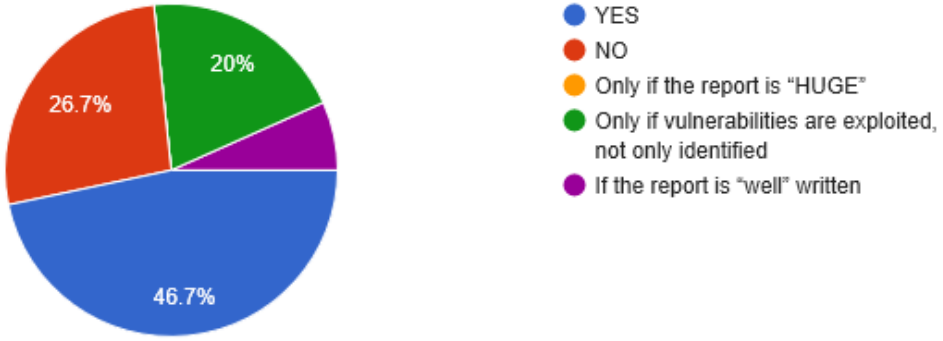


What is your conclusion after evaluation a report with low number of finding or low risk findings only?

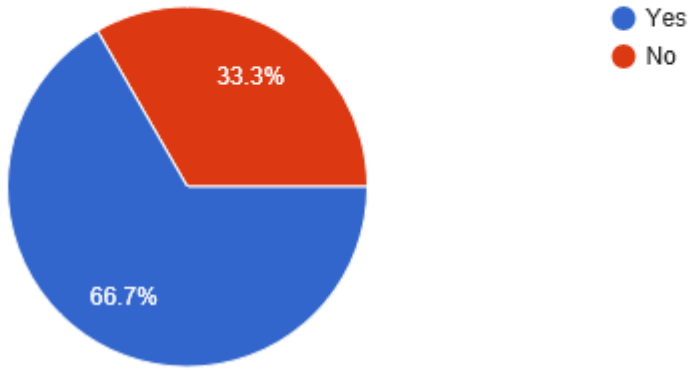


PENETRATION TESTING

Do you believe that a third party can evaluate how a penetration testing was performed only based on the report?



Would you provide assurance related to the level of security for a system or environment only based on the penetration testing report?



CONCLUSION OR BETTER A DEBATE START

INDEPENDENCE

Is the pen test conflicting the audit services?

What if the pen test is part of the audit?

RELIANCE

Can an auditor place reliance on a first time report with low no and low risk vulnerabilities?

Can the auditor assess the quality of the full pen test (and not juts the report)?

AUDIT OPINION, ASSURANCE

Can an auditor provide assurance only based on the pen test report?

DRIVER FOR PENETRATION TESTING IS REGULATORY REQUIREMENTS AND NOT SECURITY OR CYBER AWARENESS

Thank you !

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

kpmg.com/socialmedia

Gabriel Mihai Tanase

Director, Cyber-Security Services

KPMG in Romania

mtanase@kpmg.com