# Risk assessment and security testing: two sides of the same coin?

I. Rossenbach, Senior Security Expert

iro@cryptosec.org

20 March 2018

**Abstract –** In this short essay we will examine how close risk assessments and security tests are, their differences and the potential benefits of bringing these activities closer.

**Risk assessments** – Their goal is to establish a quantitative or qualitative estimation of risks related to a well-defined situation (such as a business processes) and recognized threats. After identifying the scope (processes, assets and supporting assets & processes) traditional risk assessment exercise includes five phases[1]:

- Identify threat sources and events
- Identify vulnerabilities and predisposition conditions
- Determine likelihood of occurrence
- Determine magnitude of impact
- Determine risks

The most common way to assess a risk level is to use a matrix based on likelihood of occurrence and magnitude of impact such as this one:

| Probability | Severity of Impact/Consequences | | | |
|---|---|---|---|---|
| | | Minor | Moderate | Major |
| | Frequent | Medium | High | High |
| | Likely | Low | Medium | High |
| | Remote | Insignificant | Low | Medium |

Security tests are not required in any of the above mentioned steps, even if penetration tests or vulnerability scans outcomes can provide valuable inputs for the first two phases. Instead, security experts in charge of risk assessments usually rely on generic scenarios, threat intelligence, analysis of past events, analysis of attackers TTPs (Tactics, Techniques and Procedures), or even enumerations like CAPEC[2].

There are a lot of methodologies, like ISO/IEC 27005:2011, ERM frameworks, NIST frameworks, EBIOS, etc. Usually these frameworks are customized and aligned with internal processes. None of them, however, allow unexperienced security experts to perform relevant risk assessments.

**Security testing –** Basically, security tests are meant to discover, and fix, weaknesses before threat actors do (using the same tools and techniques). They also contribute to the definition of new security controls: offence guides defense[3]. According to modern definitions[4], security tests can be classified in four categories:

- Vulnerability assessments
- Penetration tests (white, grey or black box)
- Scenario based testing (white or grey box)
- Red teaming

To this list can be added: social engineering tests, on-site audits, code audit and some other activities.

Formal security testing methodologies, frameworks and hands-on guides (OWASP, PCI, NIST, etc.) are less used than for risk assessments. Manual security tests require a high level of skills and experience. Nevertheless, penetration testers also use and rely on automated tools (fuzzing, port / service scans, site crawling, injection attempts, brute force attempts, etc.). Without these tools, coding script or *ad hoc* tools would significantly increase security testing costs and durations. Nowadays, a lot of advanced exploitation tools and frameworks exist (such as Metasploit, Core Impact, Mimikatz, BeEF, John the Ripper, etc.). These tools allow going beyond a sole vulnerability discovery in a relatively easy way. It is possible to automate some post-compromission actions to establish if a given identified vulnerability can successfully be exploited in real-world conditions (the risk situation changes if a vulnerability is easily exploitable and / or public exploits are available).

Security testing activities produce factual and reproducible findings. At the end of any kind of security testing activity the last step consist in a risk assessment. This is a key phase during which a technical finding is inserted within a business context, and then assessed, for instance, as a "low", "medium" or "high" risk. The first phase of a typical penetration test, definition of "attack scenarios", also requires some kind of risk assessment.

Risk assessments can be done without any technical testing, but any kind of security testing needs, at least, a contextualisation of its findings (and ideally a full-fledged risk assessment).

**Risk management** – Risk management aims at continuously improving security, not only by mitigating vulnerabilities but also by knowing and controlling risks, and reporting to executive management and other stakeholders.

Both risk assessments and security tests contribute to operational risk management (ORM), which is the identification, evaluation, and prioritization of risks followed by actions to reduce, avoid, transfer or accept risks (all of which are implemented in order to avoid the

[1] According to NIST definition, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. SANS propose a similar approach (https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76) and "ISO/IEC 27005:2011, Information security risk management" also: Risk identification (what can happen, when, where, how and why), Risk analysis (likelihood, consequences, risk level estimation), Risk evaluation (identify and assess options, establish priorities). CORAS method is also not far away of these core principles (http://coras.sourceforge.net)

[2] Common Attack Pattern Enumeration and Classification: https://capec.mitre.org/

[3] This is the core principle behind recognized security guidelines like CIS CSC.

[4] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

actual exploitation of a risk… unless of course while performing controlled testing activities).
Assuming that the goal is to move from a reactive security posture to a more proactive one, the next step would be to consider how risk assessment and security tests can benefit from one another.
The following table shows a list of common points and differences:

| | | Risk assessment | Security testing |
|---|---|---|---|
| 1 | Level of skills required | Intermediate | High |
| 2 | Definition of "attack scenarios" | Yes | Yes |
| 3 | Identification of weaknesses | Yes | Yes |
| 4 | Factual and reproducible findings | No | Yes |
| 5 | Check if possible exploitation | No | Possible |
| 6 | Likelihood assessment | Yes | No* |
| 7 | Impact assessment | Yes | Yes |
| 8 | Followed by an action plan | Yes | Yes |

* The risk level associated to a vulnerability significantly increase if a public exploit is available, which is analogous to a likelihood assessment.

**Possible improvements –** From these differences we can identify several axis for improvement:

**Improve quality of risk assessment findings** (row #1 and #4): In order to increase the quality of risk assessments findings, *security experts with security test skills should be involved*. Not only do they have the required specific technical skills, but they also often have the necessary "attack" mind-set to think "out of the box".
Methods used to perform risk assessments could learn from the penetration testing empirical *"try and fail" approach*. Instead of listing all possible weaknesses and then trying to associate the likelihood of it being exploited (without any relevant statistics), this different approach consists in challenging each finding and to *keep only those which are realistic from an attacker perspective.* This is typically done while running a "scenario risk assessment[5]", where the outcome is not a list of weaknesses but a list of *possible attack scenarios*[6].

**Solve the likelihood issue** (row #6): Quantitative assessment of the likelihood of a finding is almost impossible when statistics are unavailable. Furthermore, the conventional likelihood / impact matrix suffers from a major problem: the inadequate risk evaluation when there is a high impact but a low likelihood. Typically, this kind of risk is assessed as "medium". However, a "high" impact should not result in a "medium" risk[7]. Two possible improvements are: 1/ *abandon likelihood assessments when no statistics are available*, just as security tests findings assessments – 2/ *define a set of unwanted events, whatever the likelihood can be*.

**Investigate findings exploitation** (row #5): When a vulnerability is discovered during a penetration test, it is usually possible to try exploiting it. Success or failure will help to assess the risk: exploitable vulnerabilities represent a higher risk. This method should also be used with risk assessments: *whenever possible, risk assessment findings should be technically tested*.

**Merge risk assessments and security testing results presentation and follow-up** (row #8): As both activities are dedicated to identify weaknesses and define actions plans to fix them, *a common vocabulary, formalism and metrics (like CVSS) should be agreed upon and used to present and follow-up on results*. This can also help to define *global tactical and strategical way forwards* (like launching new security projects, modifying set of policies, etc.), or to provide comprehensive *security indicators*. This merge would also *make it easier to trigger technical tests after risk reduction measures are implemented* (action plan following risk assessments).

**Focus security tests on realistic threats and business process / data** (row #2): These last years, several initiatives in the financial sector like C-RAF[8] or CBEST[9] have defined how to *run risk analysis and consider threat intelligence inputs before running security tests.* The overall goal is basically to bring security tests *closer to business risks and challenges.*

**Strengthen business oriented assessment of security tests** (row #7): Security tests are more technical than risk assessments. Therefore, a valuable improvement can be to set security tests goals and assess their results taking into consideration the business context, its implications and any data oriented risk analysis available. *Risk assessment methods and results can be used to improve contextualization of security tests*. A way to achieve this, as mentioned above, is to *merge the risk assessment methodology with existing security testing framework.*

Finally, after merging both activities within a single *"cyber-risk management framework"* it will be possible to choose the relevant kind of "*risk analysis"* when needed (new component introduced in the IT infrastructure, modification of the threat landscape, after a certain period of time, etc.) among a *unified and comprehensive set of "risk analysis",* depending on resources, costs and assets / process criticality. The following table is a sample of criteria which can help to make this kind of choice:

| | Effort / Cost | Relevance of findings |
|---|---|---|
| Lightweight risk assessment | + | + |
| Comprehensive risk assessment | ++ | ++ |
| Vulnerability assessment | ++ | +++ |
| Penetration tests | +++ | +++ |
| Scenario based testing | +++ | ++++ |
| Red teaming | ++++ | +++ |
| Code audit | ++++ | ++++ |

**Conclusion**
Bring closer methods, processes and the organisation of traditional risk assessments and security tests can improve both activities. Furthermore, unification within a common "cyber-risk management framework" can significantly increase the overall proactive security posture of an organisation.

[5] "Scenario risk assessment" is the risk assessment method recommended by SWIFT's Customer Security Programme (Control 7.4A)
[6] See also "The Diamond Model of Intrusion Analysis", http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
[7] This is called a « Black Swann »: The Black Swan: The Impact of the Highly Improbable, by Nassim Nicholas Taleb.
[8] Cyber-Resilience Assessment Framework, from HKMA
[9] CBEST Vulnerability Testing Framework , leaded by the Bank of England