TIPS FOR CREATING AN INFORMATION SECURITY ASSESSMENT REPORT

This cheat sheet presents recommendations for creating a strong report as part of an information security assessment project.

General Approach to Creating the Report

1. Analyze the data collected during the security assessment to identify relevant issues.
2. Prioritize your risks and observations; formulate remediation steps.
3. Document the sections of the report detailing the assessment methodology and scope.
4. Document the sections of the report describing your findings and recommendations.
5. Attach relevant figures and raw data to support the main body of the report.
6. Create the executive summary to highlight the key findings and recommendations.
7. Proof-read and edit the document.
8. Consider submitting the report's draft to weed out false positives and confirm expectations.
9. Submit the final report to the intended recipient using agreed-upon secure transfer mechanism.
10. Discuss the report's contents with the recipient on the phone or in person.

Analysis of the Security Assessment Data

Your analysis should provide value beyond regurgitating the data already in existence.

Consider what information provided to you is incomplete or might be a lie or half-truth.

Group initial findings based on affected resources, risk, issue category, etc. to look for patterns.

Identify for trends that highlight the existence of underlying problems that affect security.

If examining scanner output, consider exploring the data using spreadsheets and pivot tables.

Fill in the gaps in your understanding with follow-up scans, document requests and/or interviews.

Involve colleagues in your analysis to obtain other people's perspectives on the data and conclusions.

Assessment Methodology Documentation

Document the methodology used to perform the assessment, analyze data and prioritize findings.

The methodology's description need to demonstrate a systemic and well-reasoned assessment approach.

Clarify the type of the assessment performed: penetration test, vulnerability assessment, etc.

If applicable, explain what security assessment tools were used and how they were configured.

If applicable, describe what approach guided the questions you asked during interviews.

Describe the criteria used to assign severity or criticality levels to the findings of the assessment.

Refer to the relevant frameworks you used to guide the assessment efforts (PCI DSS, ISO 27001, etc.).

Scope of the Security Assessment

Specify what systems, networks and/or applications were reviewed as part of the security assessment.

State what documentation was reviewed if any.

List the people whom you interviewed, if any.

Clarify the primary goals of the assessment project.

Discuss what contractual obligations or regulatory requirements were accounted for in the assessment.

Document any items that were specifically excluded from the assessment's scope and explain why.

Documenting Conclusions

Include both negative and positive findings.

Account for organization's industry, business model and compliance requirements where appropriate.

Stay consistent with the methodology and scope.

Prioritize findings related to security risks.

Provide practical remediation path, accounting for the organization's strengths and weaknesses.

Qualities of a Good Assessment Report

Starts with a strong executive summary that a non-technical reader can understand

Provides meaningful analysis, rather than merely presenting the output of assessment tools

Includes supporting figures to support the analysis

Describes assessment methodology and scope

Looks professional and is without typos

Offers remediation guidance beyond merely pointing out security problems

Is structured in logical sections to accommodate the different groups who'll read and act upon it

Additional Assessment Report Tips

Create templates based on prior reports, so you don't have to write every document from scratch.

Safeguard (encrypt) the report when storing and sending it, since its contents are probably sensitive.

Use concrete statements; avoid passive voice.

Explain the significance of the security findings in the context of current threats and events.

Put effort into making the report as brief as possible without omitting important and relevant contents.

More Security Assessment Tips

6 Qualities of a Good Information Security Report: http://j.mp/m3AK9r

4 Tips for a Strong Executive Summary of a Security Assessment Report: http://j.mp/jsT669

Security Assessment Report as Critique, Not Criticism: http://j.mp/m6e6p0

4 Reasons Why Security Assessment Recommendations Get Ignored: http://j.mp/irFHRa

Dealing with Misinformation During Security Assessments: http://j.mp/jv8jxz

Authored Lenny Zeltser, who writes a daily security blog at blog.zeltser.com; you can also find him on Twitter as @lennyzeltser. This cheat sheet was reviewed by Dave Shackleford and John Strand. You're looking at version 1.0 of this document. For more security cheat sheets see http://j.mp/mrGgHJ.