Vulnerability Remediation

QUICK EXPLORATORY SELF-ASSESSMENT GUIDE



PRACTICAL TOOLS FOR SELF-ASSESSMENT

Diagnose projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices

Implement evidence-based best practice strategies aligned with overall goals

Integrate recent advances and process design strategies into practice according to best practice guidelines

Use the Self-Assessment tool Scorecard and develop a clear picture of which areas need attention

The Art of Service

Vulnerability Remediation
Quick Exploratory Self-Assessment Guide

This Vulnerability Remediation Quick Exploratory Self-Assessment Guide is an excerpt of the Complete Vulnerability Remediation Self-Assessment guide, read more at:

https://store.theartofservice.com/

The guidance in this Self-Assessment is based on Vulnerability Remediation best practices and standards in business process architecture, design and quality management. The guidance is also based on the professional judgment of the individual collaborators listed in the Acknowledgments.

Table of Contents

About The Art of Service

The Art of Service, Business Process Architects since 2000, is dedicated to helping stakeholders achieve excellence.

Defining, designing, creating, and implementing a process to solve a business challenge or meet a stakeholder objective is the most valuable role… In EVERY company, organization and department.

Unless you're talking a one-time, single-use project within a group, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions.

Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?'

With The Art of Service's Standard Requirements Self-Assessments, we empower people who can do just that — whether their title is marketer, entrepreneur, manager, salesperson, consultant, Business Process Manager, executive assistant, IT Manager, CIO etc... —they are the people who rule the future. They are people who watch the process as it happens, and ask the right questions to make the process work better.

Contact us when you need any support with this Self-Assessment and any help with templates, blue-prints and examples of standard documents you might need:

https://theartofservice.com
support@theartofservice.com

Complete Resources - how to access

The Complete Vulnerability Remediation Self-Assessment Guide

includes ALL questions and Self-Assessment areas.

Included are all the Vulnerability Remediation Self-Assessment questions in a ready to use Excel spreadsheet, containing the self-assessment, graphs, and project RACI planning - all with examples to get you started right away. Go to:

https://store.theartofservice.com

Purpose of this Self-Assessment

This Self-Assessment has been developed to improve understanding of the requirements and elements of Vulnerability Remediation, based on best practices and standards in business process architecture, design and quality management.

It is designed to allow for a rapid Self-Assessment of an organization or facility to determine how closely existing management practices and procedures correspond to the elements of the Self-Assessment.

The criteria of requirements and elements of Vulnerability Remediation have been rephrased in the format of a Self-Assessment questionnaire, with a seven-criterion scoring system, as explained in this document.

In this format, even with limited background knowledge of Vulnerability Remediation, a manager can quickly review existing operations to determine how they measure up to the standards. This in turn can serve as the starting point of a 'gap analysis' to identify management tools or system elements that might usefully be implemented in the organization to help improve overall performance.

How to use the Self-Assessment

On the following pages are a series of questions to identify to what extent your Vulnerability Remediation initiative is complete in comparison to the requirements set in standards.

To facilitate answering the questions, there is a space in front of each question to enter a score on a scale of '1' to '5'.

1 Strongly Disagree

2 Disagree

3 Neutral

4 Agree

5 Strongly Agree

Read the question and rate it with the following in front of mind:

'In my belief,
the answer to this question is clearly defined'.

There are two ways in which you can choose to interpret this statement;

1. how aware are you that the answer to the question is clearly defined
2. for more in-depth analysis you can choose to gather evidence and confirm the answer to the question. This obviously will take more time, most Self-Assessment users opt for the first way to interpret the question and dig deeper later on based on the outcome of the overall Self-Assessment.

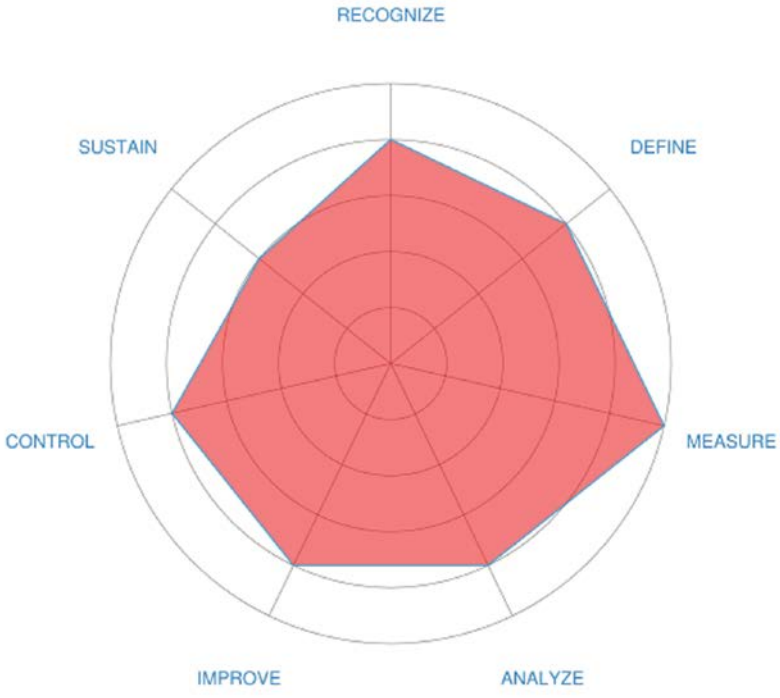
A score of '1' would mean that the answer is not clear at all, where a '5' would mean the answer is crystal clear and defined. Leave emtpy when the question is not applicable or you don't want to answer it, you can skip it without affecting your score. Write your score in the space provided.

After you have responded to all the appropriate statements in each section, compute your average score for that section, using the formula provided, and round to the nearest tenth. Then transfer to the corresponding spoke in the Vulnerability Remediation Scorecard on the second next page of the Self-Assessment.

Your completed Vulnerability Remediation Scorecard will give you a clear presentation of which Vulnerability Remediation areas need attention.

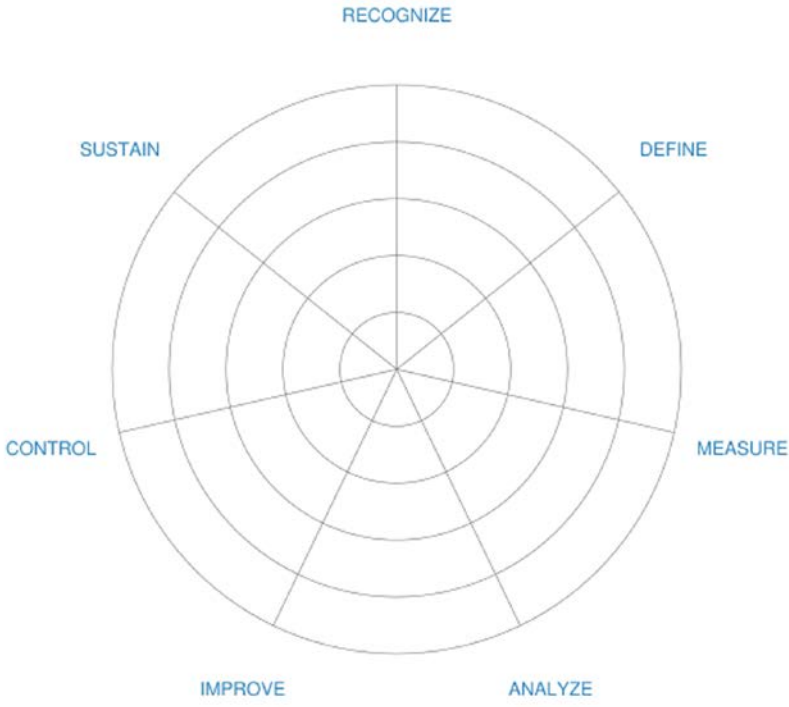
Vulnerability Remediation Scorecard Example

Example of how the finalized Scorecard can look like:



Vulnerability Remediation Scorecard

Your Scores:



SELF-ASSESSMENT SECTION START

BEGINNING OF THE SELF-ASSESSMENT:

CRITERION #1: RECOGNIZE

INTENT: Be aware of the need for change. Recognize that there is an unfavorable variation, problem or symptom.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. Are vulnerability scanning tools run on the incident management systems and networks?
<--- Score

2. What is remediation orchestration?
<--- Score

3. Are defects and weaknesses tracked from discovery and notification through to

remediation?
<--- Score

4. When was the last security or vulnerability assessment conducted?
<--- Score

5. Are systems and applications periodically scanned for common and new vulnerabilities?
<--- Score

6. Why would your organization fix the least important vulnerabilities the most often?
<--- Score

7. Who has responsibility for vulnerability management currently within your organization?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Vulnerability Remediation Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #2: DEFINE:

INTENT: Formulate the stakeholder problem. Define the problem, needs and objectives.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. What would be the scope of the program?
<--- Score

2. Does absolute reach require connection to the corporate network to be effective?
<--- Score

3. What are your compliance requirements?
<--- Score

4. How do you determine your validation requirements?
<--- Score

5. Does your organization duty to protect mostly just require more regulation?
<--- Score

6. Are there any regulatory requirements pertaining to the application?
<--- Score

7. Does the software require authorization when it should?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Vulnerability Remediation Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #3: MEASURE:

INTENT: Gather the correct data.
Measure the current performance and
evolution of the situation.

In my belief, the answer to this
question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. How much would one hour of downtime cost your business?
<--- Score

2. Does your organization share the cost risk identification measures with suppliers?
<--- Score

3. Does a new policy outweigh the cost of all breaches put together?

<--- Score

4. Is per project data for the cost of assurance activities collected?
<--- Score

5. Do you need to reduce your overall cost of compliance?
<--- Score

6. How do you assist / define remediation prioritization?
<--- Score

7. How is vulnerability remediation prioritized?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Vulnerability Remediation Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #4: ANALYZE:

INTENT: Analyze causes, assumptions and hypotheses.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. What parts of your organization do you remediate quickly and what parts will take longer?
<--- Score

2. Are higher severity vulnerabilities patched quicker?
<--- Score

3. Which team is responsible for each stage of the security vulnerability remediation process?
<--- Score

4. How can security and IT teams collaborate on the remediation process?
<--- Score

5. How is the flaw remediation process managed?
<--- Score

6. What products and services are required to adopt the security development lifecycle process?
<--- Score

7. Are service releases required to adopt the security development lifecycle process?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Vulnerability Remediation Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #5: IMPROVE:

INTENT: Develop a practical solution. Innovate, establish and test the solution and to measure the results.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. Where and how much do you need to invest to optimize your cyber capabilities?
<--- Score

2. Does the vendor offer services for deployment and optimization?
<--- Score

3. Is your goal to optimize production?
<--- Score

4. Are there clearly defined criteria for remediation of security risk for commercialized product?
<--- Score

5. What are the risks to your business?
<--- Score

6. What level of risk are the adversaries likely to accept?
<--- Score

7. Are the adversaries willing to risk getting caught?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Vulnerability Remediation Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #6: CONTROL:

INTENT: Implement the practical solution. Maintain the performance and correct possible complications.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. What is your level of resilience against cyberattacks?
<--- Score

2. Is all xml input data validated against an agreed schema?
<--- Score

3. Do project teams check software designs against known security risks?

<--- Score

4. Are audits performed against the security requirements specified by project teams?
<--- Score

5. Does your monitoring process also identify risks to business?
<--- Score

6. How is access assigned, approved, monitored, and removed?
<--- Score

7. Has your organization established a continuous monitoring of impacts?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Vulnerability Remediation Index at the beginning of the Self-Assessment.

CRITERION #7: SUSTAIN:

INTENT: Retain the benefits.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. Have new benefits been realized?
<--- Score

2. Are new benefits received and understood?
<--- Score

3. Were lessons learned captured and communicated?
<--- Score

4. Have benefits been optimized with all key stakeholders?
<--- Score

5. What do we do when new problems arise?
<--- Score

6. How does Vulnerability Remediation integrate with other stakeholder initiatives?
<--- Score

7. Is the impact that Vulnerability Remediation has shown?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Vulnerability Remediation Index at the beginning of the Self-Assessment.

Index