

# 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.

### **Notice of rights**

**You are licensed to use the Self-Assessment contents in your presentations and materials for internal use and customers without asking us - we are here to help.**

All rights reserved for the book itself: this book may not be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. The information in this book is distributed on an "As Is" basis without warranty. While every precaution has been taken in the preparation of the book, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the products described in it.

### **Trademarks**

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.

Copyright © by The Art of Service  
<https://theartofservice.com>  
[support@theartofservice.com](mailto:support@theartofservice.com)

# Table of Contents

---

About The Art of Service	3
Complete Resources - how to access	3
Purpose of this Self-Assessment	4
How to use the Self-Assessment	4
Vulnerability Remediation	
Scorecard Example	7
Vulnerability Remediation	
Scorecard	8
BEGINNING OF THE	
SELF-ASSESSMENT:	10
CRITERION #1: RECOGNIZE	11
CRITERION #2: DEFINE:	14
CRITERION #3: MEASURE:	17
CRITERION #4: ANALYZE:	20
CRITERION #5: IMPROVE:	23
CRITERION #6: CONTROL:	26
CRITERION #7: SUSTAIN:	28
Index	30

# About The Art of Service

---

**T**he 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](mailto: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.

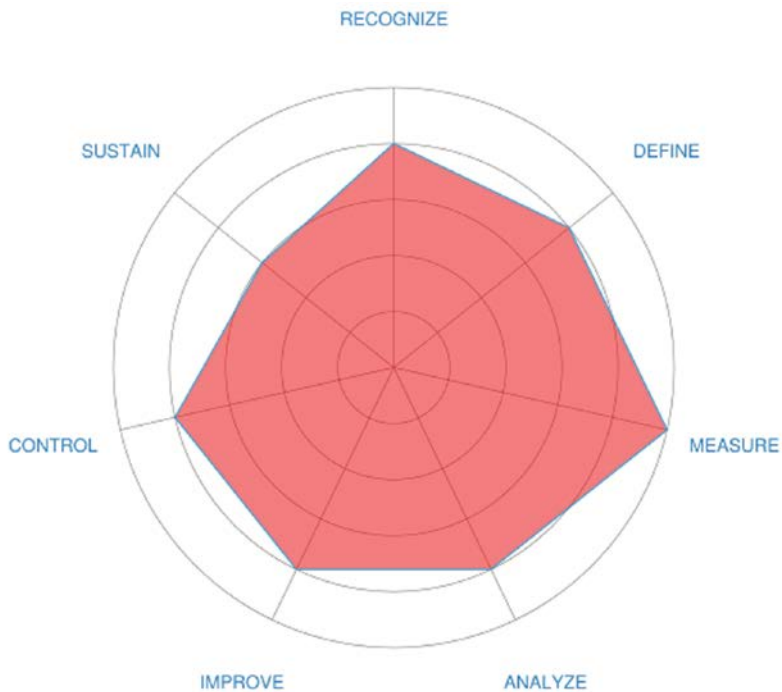
A score of '1' would mean that the answer is not clear at all, where a '5' would mean the answer is crystal clear and defined. Leave empty when the question is not applicable or you don't want to answer it, you can skip it without affecting your score. Write your score in the space provided.

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:

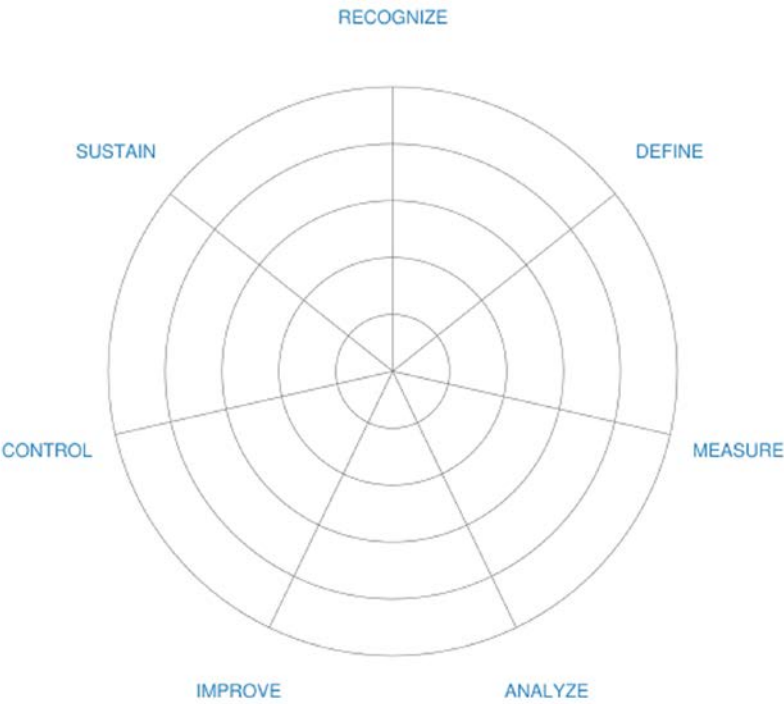




# Vulnerability Remediation Scorecard

---

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

---

absolute	14
accept	24
access	2-3, 27
accomplish	3
achieve	3
activities	18
affecting	5
against	26-27
agreed	26
alleged	1
analysis	4-5
ANALYZE	2, 20
answer	5, 11, 14, 17, 20, 23, 26, 28
answered	12, 15, 18, 21, 24, 27, 29
answering	5
appear	1
applicable	5
approved	27
Architects	3
asking	1, 3
assessment	12
assigned	27
assist	18
assistant	3
assurance	18
attention	6
audits	27
author	1
Average	6, 12, 15, 18, 21, 24, 27, 29
background	4
beginning	2, 10, 12, 15, 18, 21, 24, 27, 29
belief	5, 11, 14, 17, 20, 23, 26, 28
benefit	1
benefits	28
better	3
breaches	17
business	1, 3-4, 17, 24, 27
capable	3
captured	28
caught	24

caused	1
causes	20
challenge	3
change	11
choose	5
claimed	1
clearly	5, 11, 14, 17, 20, 23-24, 26, 28
closely	4
collected	18
common	12
companies	1
company	3
comparison	5
Complete	1-3, 5
completed	6
complex	3
compliance	14, 18
compute	6
conducted	12
confirm	5
connection	14
consultant	3
Contact	3
contained	1
containing	4
Contents	1-2
continuous	27
CONTROL	2, 26
convey	1
Copyright	1
corporate	14
correct	17, 26
correspond	4
creating	3
criteria	4, 24
CRITERION	2, 11, 14, 17, 20, 23, 26, 28
crystal	5
current	17
currently	12
customers	1
damage	1
dedicated	3
deeper	5



defects	11
DEFINE	2, 14, 18
defined	5, 11, 14, 17, 20, 23-24, 26, 28
Defining	3
department	3
deployment	23
described	1
design	1, 4
designed	3-4
designing	3
designs	26
determine	4, 15
Develop	23
developed	4
different	3
directly	1
Disagree	5, 11, 14, 17, 20, 23, 26, 28
discovery	11
Divided	12, 15, 18, 21, 24, 27, 29
document	4
documents	3
downtime	17
editorial	1
effective	14
electronic	1
elements	4
empower	3
enough	3
entity	1
establish	23
evidence	5
evolution	17
Example	2, 7
examples	3-4
excellence	3
excerpt	1
executive	3
existing	4
explained	4
extent	5
facilitate	5
facility	4
fashion	1

finalized	7
following	5
format	4
formula	6
Formulate	14
future	3
Gather	5, 17
getting	24
graphs	4
guidance	1
happens	3
helping	3
higher	20
humans	3
hypotheses	20
identified	1
identify	4-5, 27
impact	29
impacts	27
Implement	26
important	12
IMPROVE	2, 4, 23
incident	11
Included	4
includes	4
in-depth	5
indirectly	1
individual	1
initiative	5
Innovate	23
integrate	29
intended	1
INTENT	11, 14, 17, 20, 23, 26, 28
intention	1
internal	1
interpret	5
invest	23
itself	1
judgment	1
knowledge	4
learned	28
lessons	28
liability	1

licensed	1
lifecycle	21
likely	24
limited	4
listed	1
longer	20
Maintain	26
managed	3, 21
management	1, 4, 11-12
manager	3-4
marketer	3
materials	1
measure	2, 4, 17, 23
measures	17
mechanical	1
monitored	27
monitoring	27
mostly	15
nearest	6
neither	1
network	14
networks	11
Neutral	5, 11, 14, 17, 20, 23, 26, 28
Notice	1
number	12, 15, 18, 21, 24, 27, 29-30
objective	3
objectives	14
obviously	5
one-time	3
operations	4
optimize	23
optimized	28
otherwise	1
outcome	5
outweigh	17
overall	4-5, 18
patched	20
people	3
performed	27
permission	1
person	1
pertaining	15
planning	4

points 12, 15, 18, 21, 24, 27, 29  
 policy 17  
 possible 26  
 practical 23, 26  
 practices 1, 4  
 precaution 1  
 problem 11, 14  
 problems 29  
 procedures 4  
 process 1, 3-4, 20-21, 27  
 product 1, 24  
 production 23  
 products 1, 21  
 program 14  
 project 3-4, 18, 26-27  
 protect 15  
 provided 5-6  
 publisher 1  
 Purpose 2, 4  
 quality 1, 4  
 question 5, 11, 14, 17, 20, 23, 26, 28  
 questions 3-5  
 quicker 20  
 quickly 4, 20  
 realized 28  
 really 3  
 received 28  
 RECOGNIZE 2, 11  
 recording 1  
 reduce 18  
 references 30  
 regulation 15  
 regulatory 15  
 releases 21  
 remediate 20  
 removed 27  
 rephrased 4  
 reproduced 1  
 requested 1  
 require 14-15  
 required 21  
 reserved 1  
 resilience 26

Resources	2-3
respect	1
responded	6
results	23
Retain	28
review	4
rights	1
scanned	12
scanning	11
schema	26
Scorecard	2, 6-8
Scores	8
scoring	4
second	6
section	6, 12, 15, 18, 21, 24, 27, 29
security	12, 20-21, 24, 26-27
sellers	1
series	5
Service	1-3, 21
services	1, 21, 23
severity	20
should	3, 15
single-use	3
situation	17
software	15, 26
solution	23, 26
Someone	3
specified	27
standard	3
standards	1, 4-5
started	4
starting	4
statement	5
statements	6, 12, 15, 18, 21, 24, 27, 29
Strongly	5, 11, 14, 17, 20, 23, 26, 28
suppliers	17
support	1, 3
SUSTAIN	2, 28
symptom	11
system	4
systems	11-12
talking	3
templates	3

through	11
throughout	1
together	17
tracked	11
trademark	1
trademarks	1
Transfer	6, 12, 15, 18, 21, 24, 27, 29
trying	3
understood	28
Unless	3
usefully	4
validated	26
validation	15
valuable	3
variation	11
vendor	23
Version	30
warranty	1
weaknesses	11
whether	3
willing	24
within	3, 12
without	1, 5
written	1