Vulnerability Remediation

COMPLETE 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

"After utilizing toolkits from The Art of Service, I was able to identify threats within my organization to which I was completely unaware. Using my team's knowledge as a competitive advantage, we now have superior systems that save time and energy."

"As a new Chief Technology Officer, I was feeling unprepared and inadequate to be successful in my role. I ordered an IT toolkit Sunday night and was prepared Monday morning to shed light on areas of improvement within my organization. I no longer felt overwhelmed and intimidated, I was excited to share what I had learned."

"I used the questionnaires to interview members of my team. I never knew how many insights we could produce collectively with our internal knowledge."

"I usually work until at least 8pm on weeknights. The Art of Service questionnaire saved me so much time and worry that Thursday night I attended my son's soccer game without sacrificing my professional obligations."

"After purchasing The Art of Service toolkit, I was able to identify areas where my company was not in compliance that could have put my job at risk. I looked like a hero when I proactively educated my team on the risks and presented a solid solution."

"I spent months shopping for an external consultant before realizing that The Art of Service would allow my team to consult themselves! Not only did we save time not catching a consultant up to speed, we were able to keep our company information and industry secrets confidential."

"Everyday there are new regulations and processes in my industry. The Art of Service toolkit has kept me ahead by using AI technology to constantly update the toolkits and address emerging needs."

"I customized The Art of Service toolkit to focus specifically on the concerns of my role and industry. I didn't have to waste time with a generic self-help book that wasn't tailored to my exact situation."

"Many of our competitors have asked us about our secret sauce. When I tell them it's the knowledge we have in-house, they never believe me. Little do they know The Art of Service toolkits are working behind the scenes."

"One of my friends hired a consultant who used the knowledge gained working with his company to advise their competitor. Talk about a competitive disadvantage! The Art of Service allowed us to keep our knowledge from walking out the door along with a huge portion of our budget in consulting fees."

"Honestly, I didn't know what I didn't know. Before purchasing The Art of Service, I didn't realize how many areas of my business needed to be refreshed and improved. I am so relieved The Art of Service was there to highlight our blind spots."

"Before The Art of Service, I waited eagerly for consulting company reports to come out each month. These reports kept us up to speed but provided little value because they put our competitors on the same playing field. With The Art of Service, we have uncovered unique insights to drive our business forward."

"Instead of investing extensive resources into an external consultant, we can spend more of our budget towards pursuing our company goals and objectives…while also spending a little more on corporate holiday parties."

"The risk of our competitors getting ahead has been mitigated because The Art of Service has provided us with a 360-degree view of threats within our organization before they even arise."

Vulnerability Remediation
Complete Self-Assessment Guide

Table of Contents

About The Art of Service 8
Included Resources - how to access 9
Purpose of this Self-Assessment 10
How to use the Self-Assessment 11
Vulnerability Remediation Scorecard Example 13
Vulnerability Remediation Scorecard 14

BEGINNING OF THE SELF-ASSESSMENT: 17
CRITERION #1: RECOGNIZE 18
CRITERION #2: DEFINE: 29
CRITERION #3: MEASURE: 43
CRITERION #4: ANALYZE: 54
CRITERION #5: IMPROVE: 69
CRITERION #6: CONTROL: 85
CRITERION #7: SUSTAIN: 100
Vulnerability Remediation and Managing Projects, Criteria for Project Managers: 145
1.0 Initiating Process Group: Vulnerability Remediation 146
1.1 Project Charter: Vulnerability Remediation 148
1.2 Stakeholder Register: Vulnerability Remediation 150
1.3 Stakeholder Analysis Matrix: Vulnerability Remediation 151
2.0 Planning Process Group: Vulnerability Remediation 153
2.1 Project Management Plan: Vulnerability Remediation 155
2.2 Scope Management Plan: Vulnerability Remediation 157
2.3 Requirements Management Plan: Vulnerability Remediation 159
2.4 Requirements Documentation: Vulnerability Remediation 161
2.5 Requirements Traceability Matrix: Vulnerability Remediation 163
2.6 Project Scope Statement: Vulnerability Remediation 165
2.7 Assumption and Constraint Log: Vulnerability Remediation 167

2.8 Work Breakdown Structure: Vulnerability Remediation 169
2.9 WBS Dictionary: Vulnerability Remediation 171
2.10 Schedule Management Plan: Vulnerability Remediation 174
2.11 Activity List: Vulnerability Remediation 176
2.12 Activity Attributes: Vulnerability Remediation 178
2.13 Milestone List: Vulnerability Remediation 180
2.14 Network Diagram: Vulnerability Remediation 182
2.15 Activity Resource Requirements: Vulnerability Remediation 184
2.16 Resource Breakdown Structure: Vulnerability Remediation 185
2.17 Activity Duration Estimates: Vulnerability Remediation 187
2.18 Duration Estimating Worksheet: Vulnerability Remediation 189
2.19 Project Schedule: Vulnerability Remediation 191
2.20 Cost Management Plan: Vulnerability Remediation 193
2.21 Activity Cost Estimates: Vulnerability Remediation 195
2.22 Cost Estimating Worksheet: Vulnerability Remediation 197
2.23 Cost Baseline: Vulnerability Remediation 199
2.24 Quality Management Plan: Vulnerability Remediation 201
2.25 Quality Metrics: Vulnerability Remediation 203
2.26 Process Improvement Plan: Vulnerability Remediation 205
2.27 Responsibility Assignment Matrix: Vulnerability Remediation 207
2.28 Roles and Responsibilities: Vulnerability Remediation 209
2.29 Human Resource Management Plan: Vulnerability Remediation 211
2.30 Communications Management Plan: Vulnerability Remediation 213
2.31 Risk Management Plan: Vulnerability Remediation 215
2.32 Risk Register: Vulnerability Remediation 217

2.33 Probability and Impact Assessment: Vulnerability Remediation 219
2.34 Probability and Impact Matrix: Vulnerability Remediation 221
2.35 Risk Data Sheet: Vulnerability Remediation 223
2.36 Procurement Management Plan: Vulnerability Remediation 225
2.37 Source Selection Criteria: Vulnerability Remediation 227
2.38 Stakeholder Management Plan: Vulnerability Remediation 229
2.39 Change Management Plan: Vulnerability Remediation 231
3.0 Executing Process Group: Vulnerability Remediation 233
3.1 Team Member Status Report: Vulnerability Remediation 235
3.2 Change Request: Vulnerability Remediation 237
3.3 Change Log: Vulnerability Remediation 239
3.4 Decision Log: Vulnerability Remediation 241
3.5 Quality Audit: Vulnerability Remediation 243
3.6 Team Directory: Vulnerability Remediation 246
3.7 Team Operating Agreement: Vulnerability Remediation 248
3.8 Team Performance Assessment: Vulnerability Remediation 250
3.9 Team Member Performance Assessment: Vulnerability Remediation 252
3.10 Issue Log: Vulnerability Remediation 254
4.0 Monitoring and Controlling Process Group: Vulnerability Remediation 256
4.1 Project Performance Report: Vulnerability Remediation 258
4.2 Variance Analysis: Vulnerability Remediation 260
4.3 Earned Value Status: Vulnerability Remediation 262
4.4 Risk Audit: Vulnerability Remediation 264
4.5 Contractor Status Report: Vulnerability Remediation 266
4.6 Formal Acceptance: Vulnerability Remediation 268
5.0 Closing Process Group: Vulnerability Remediation 270
5.1 Procurement Audit: Vulnerability Remediation 272
5.2 Contract Close-Out: Vulnerability Remediation 274

5.3 Project or Phase Close-Out: Vulnerability Remediation 276
5.4 Lessons Learned: Vulnerability Remediation 278
Index 280

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 stakeholders challenge or meet an objective is the most valuable role… In EVERY group, company, organization and department.

Unless you're talking a one-time, single-use project, 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 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

Included Resources - how to access

Included with your purchase of the book is the Vulnerability Remediation Self-Assessment Spreadsheet Dashboard which contains all questions and Self-Assessment areas and auto-generates insights, graphs, and project RACI planning - all with examples to get you started right away.

How? Simply send an email to
access@theartofservice.com
with this books' title in the subject to get the Vulnerability Remediation Self Assessment Tool right away.

The auto reply will guide you further, you will then receive the following contents with New and Updated specific criteria:

- The latest quick edition of the book in PDF
- The latest complete edition of the book in PDF, which criteria correspond to the criteria in...
- The Self-Assessment Excel Dashboard, and...
- Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation
- In-depth specific Checklists covering the topic
- Project management checklists and templates to assist with implementation

INCLUDES LIFETIME SELF ASSESSMENT UPDATES

Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

Get it now- you will be glad you did - do it now, before you forget.

Send an email to **access@theartofservice.com** with this books' title in the subject to get the Vulnerability Remediation Self Assessment Tool right away.

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 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

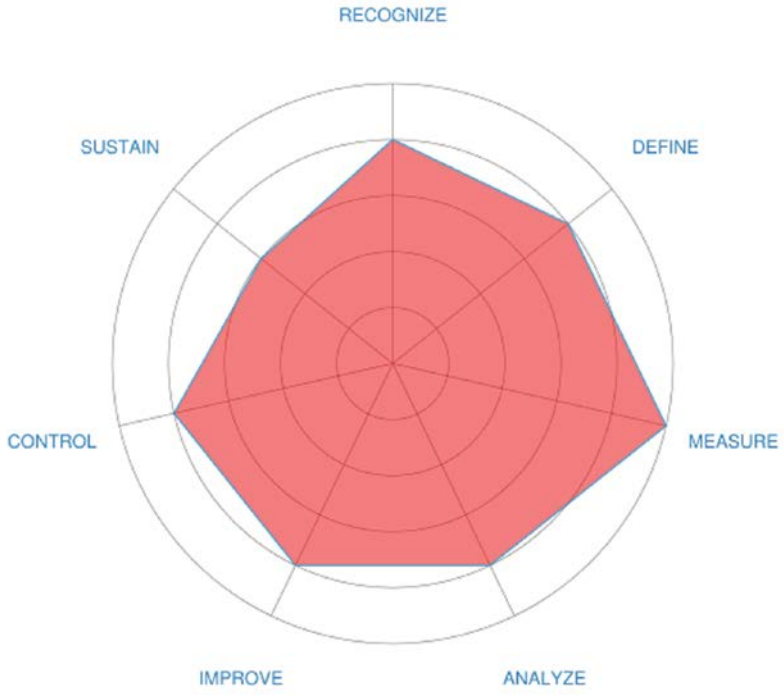
or you don't want to answer it, you can skip it without affecting your score. Write your score in the space provided.

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.

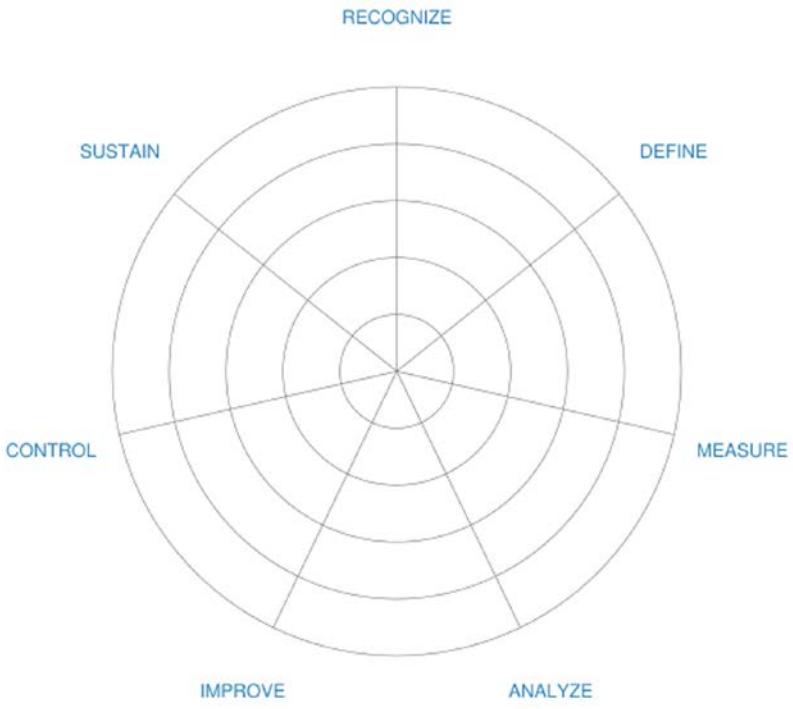
Vulnerability Remediation Scorecard Example

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. Do your employees know how to identify and respond to attacks?
<--- Score

2. When a Vulnerability Remediation manager recognizes a problem, what options are available?
<--- Score

3. What are the issues organizations should be

aware of?
<--- Score

4. Do all of your information assets need an owner?
<--- Score

5. Will a response program recognize when a crisis occurs and provide some level of response?
<--- Score

6. Can management personnel recognize the monetary benefit of Vulnerability Remediation?
<--- Score

7. How are you going to measure success?
<--- Score

8. What events should trigger automated remediation?
<--- Score

9. How much are sponsors, customers, partners, stakeholders involved in Vulnerability Remediation? In other words, what are the risks, if Vulnerability Remediation does not deliver successfully?
<--- Score

10. How do you track which updates different machines need?
<--- Score

11. What percentage of applications, users and devices has been reviewed for security issues?
<--- Score

12. Are there recognized Vulnerability Remediation problems?
<--- Score

13. What problems are you facing and how do you consider Vulnerability Remediation will circumvent those obstacles?
<--- Score

14. What systems have the info that you need?
<--- Score

15. Are Vulnerability Remediation changes recognized early enough to be approved through the regular process?
<--- Score

16. How many security issues are found during secure code reviews?
<--- Score

17. When do you issue a remediation request?
<--- Score

18. How did you handle legal compliance issues in the beginning?
<--- Score

19. Do projects have a point of contact for security issues or incidents?
<--- Score

20. How do you recognize an objection?
<--- Score

21. To what extent does each concerned units

management team recognize Vulnerability Remediation as an effective investment?
<--- Score

22. What are changes that are causing problems for IT security and operations teams?
<--- Score

23. What is the type of problem that approaches address?
<--- Score

24. Does Vulnerability Remediation create potential expectations in other areas that need to be recognized and considered?
<--- Score

25. Will you, the vendor, need to remotely log on to the system for administration or maintenance?
<--- Score

26. As a sponsor, customer or management, how important is it to meet goals, objectives?
<--- Score

27. How do you stay flexible and focused to recognize larger Vulnerability Remediation results?
<--- Score

28. Who needs to be included on the response team?
<--- Score

29. What are the main issues that stop more people from using the existing services?

<--- Score

30. Are your systems correctly configured to prevent hackers from getting in?
<--- Score

31. What situation(s) led to this Vulnerability Remediation Self Assessment?
<--- Score

32. To what extent does management recognize Vulnerability Remediation as a tool to increase the results?
<--- Score

33. Why is network security an issue?
<--- Score

34. What does Vulnerability Remediation success mean to the stakeholders?
<--- Score

35. How will you recognize and celebrate results?
<--- Score

36. Are there any specific expectations or concerns about the Vulnerability Remediation team, Vulnerability Remediation itself?
<--- Score

37. How do you most effectively communicate information about security problems?
<--- Score

38. What are the specific kinds of vulnerabilities that scanning can identify and help to remediate?

<--- Score

39. Does the application need refactoring?
<--- Score

40. What is the recognized need?
<--- Score

41. Do you need to know how to code?
<--- Score

42. Does climate adaptation policy need probabilities?
<--- Score

43. How do you recognize an Vulnerability Remediation objection?
<--- Score

44. How are the Vulnerability Remediation's objectives aligned to the group's overall stakeholder strategy?
<--- Score

45. Are controls defined to recognize and contain problems?
<--- Score

46. What are the environmental issues facing the community where you live?
<--- Score

47. Do you recognize Vulnerability Remediation achievements?
<--- Score

48. Have you identified an individual or team who

will communicate relevant news regularly?
<--- Score

49. What practices helps your organization to develop its capacity to recognize patterns?
<--- Score

50. To what extent would your organization benefit from being recognized as a award recipient?
<--- Score

51. How much personally identifiable information could be disclosed?
<--- Score

52. Who makes decisions on open source related issues?
<--- Score

53. What are the minority interests and what amount of minority interests can be recognized?
<--- Score

54. Is a discovered security vulnerability a real issue?
<--- Score

55. Are employees recognized or rewarded for performance that demonstrates the highest levels of integrity?
<--- Score

56. What good is software that cannot be relied on to operate as and when it is needed?
<--- Score

57. Are losses recognized in a timely manner?
<--- Score

58. Who else hopes to benefit from it?
<--- Score

59. Is the need for organizational change recognized?
<--- Score

60. What vulnerabilities were identified that you were unable to patch or mitigate?
<--- Score

61. What are the stakeholder objectives to be achieved with Vulnerability Remediation?
<--- Score

62. What are the expected benefits of Vulnerability Remediation to the stakeholder?
<--- Score

63. Who needs to share information, and who can resolve the issues that emerge?
<--- Score

64. Do you need to create a vulnerability management policy or update it?
<--- Score

65. What supports are available to employees who need assistance with department behavior management?
<--- Score

66. Which human rights issues may arise within your organizations sphere of influence?
<--- Score

67. Should you invest in industry-recognized qualifications?
<--- Score

68. Are employees recognized for desired behaviors?
<--- Score

69. What would happen if Vulnerability Remediation weren't done?
<--- Score

70. How much time, effort, and expertise is needed to exploit the threat?
<--- Score

71. Would you recognize a threat from the inside?
<--- Score

72. How do you prevent forced access?
<--- 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. Who are the Vulnerability Remediation improvement team members, including Management Leads and Coaches?
<--- Score

2. If substitutes have been appointed, have they been briefed on the Vulnerability Remediation goals and received regular communications as to the progress to date?
<--- Score

3. Can the cloud provider generate reports as required?
<--- Score

4. What are the rough order estimates on cost savings/ opportunities that Vulnerability Remediation brings?
<--- Score

5. What key stakeholder process output measure(s) does Vulnerability Remediation leverage and how?
<--- Score

6. Is the current 'as is' process being followed? If not, what are the discrepancies?
<--- Score

7. Is the improvement team aware of the different versions of a process: what they think it is vs. what it actually is vs. what it should be vs. what it could be?
<--- Score

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

9. Is the team formed and are team leaders (Coaches and Management Leads) assigned?
<--- Score

10. Is Vulnerability Remediation currently on schedule according to the plan?
<--- Score

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

12. Has the direction changed at all during the course of Vulnerability Remediation? If so, when did it change and why?
<--- Score

13. How is the team tracking and documenting its work?
<--- Score

14. Has anyone else (internal or external to the group) attempted to solve this problem or a similar one before? If so, what knowledge can be leveraged from these previous efforts?
<--- Score

15. How do you keep key subject matter experts in the loop?
<--- Score

16. Are different versions of process maps needed to account for the different types of inputs?
<--- Score

17. How do you define and track engagement?
<--- Score

18. Is there a completed, verified, and validated high-level 'as is' (not 'should be' or 'could be') stakeholder process map?
<--- Score

19. What critical content must be communicated – who, what, when, where, and how?
<--- Score

20. How would you define a strong security

operations program?
<--- Score

21. Are customer(s) identified and segmented according to their different needs and requirements?
<--- Score

22. Are compliance requirements specifically considered by project teams?
<--- Score

23. What is the level of effort required to address the vulnerability in its entirety?
<--- Score

24. How often are the team meetings?
<--- Score

25. When is the estimated completion date?
<--- Score

26. Has the Vulnerability Remediation work been fairly and/or equitably divided and delegated among team members who are qualified and capable to perform the work? Has everyone contributed?
<--- Score

27. How did the Vulnerability Remediation manager receive input to the development of a Vulnerability Remediation improvement plan and the estimated completion dates/times of each activity?
<--- Score

28. What are the compelling stakeholder reasons for embarking on Vulnerability Remediation?
<--- Score

29. How do you define a policy of secure configurations?
<--- Score

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

31. Will team members regularly document their Vulnerability Remediation work?
<--- Score

32. How skilled are your adversaries, and what skills are required to exploit your weaknesses?
<--- Score

33. Where are connecting clouds required?
<--- Score

34. What are the requirements for software delivered to your organization from a vendor?
<--- Score

35. Are improvement team members fully trained on Vulnerability Remediation?
<--- Score

36. Is full participation by members in regularly held team meetings guaranteed?
<--- Score

37. Has a team charter been developed and communicated?
<--- Score

38. What specifically is the problem? Where does it occur? When does it occur? What is its extent?
<--- Score

39. What constraints exist that might impact the team?
<--- Score

40. Which use cases do you want remediation to support?
<--- Score

41. Do stakeholders review vendor agreements for security requirements?
<--- Score

42. Has the improvement team collected the 'voice of the customer' (obtained feedback – qualitative and quantitative)?
<--- Score

43. How to get an insight into the content of a software code to fulfil compliance requirements?
<--- Score

44. Has a high-level 'as is' process map been completed, verified and validated?
<--- Score

45. Have the customer needs been translated into specific, measurable requirements? How?
<--- Score

46. Is data collected and displayed to better understand customer(s) critical needs and requirements.

<--- Score

47. Has/have the customer(s) been identified?
<--- Score

48. What are the boundaries of the scope? What is in bounds and what is not? What is the start point? What is the stop point?
<--- Score

49. What would be the goal or target for a Vulnerability Remediation's improvement team?
<--- Score

50. Is a fully trained team formed, supported, and committed to work on the Vulnerability Remediation improvements?
<--- Score

51. Is Vulnerability Remediation linked to key stakeholder goals and objectives?
<--- Score

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

53. When is/was the Vulnerability Remediation start date?
<--- Score

54. What are the Roles and Responsibilities for each team member and its leadership? Where is this documented?
<--- Score

55. Are all security test requirements being met?
<--- Score

56. Has everyone on the team, including the team leaders, been properly trained?
<--- Score

57. What customer feedback methods were used to solicit their input?
<--- Score

58. Is there a completed SIPOC representation, describing the Suppliers, Inputs, Process, Outputs, and Customers?
<--- Score

59. How does the Vulnerability Remediation manager ensure against scope creep?
<--- Score

60. Do all network infrastructure devices require PKI based authentication/credentials for login?
<--- Score

61. What administrative accesses are required, if any?
<--- Score

62. What are the dynamics of the communication plan?
<--- Score

63. Are security test cases comprehensively generated for application specific logic?
<--- Score

64. What are the legal, regulatory, and contractual requirements your organization must meet?
<--- Score

65. Is responsibility for the working environment clearly defined at all levels in your organization?
<--- Score

66. Are there different segments of customers?
<--- Score

67. Are stakeholder processes mapped?
<--- Score

68. Do project teams pull requirements from best practices and compliance guidance?
<--- Score

69. Are cti requirements clearly defined in your organization?
<--- Score

70. How was the 'as is' process map developed, reviewed, verified and validated?
<--- Score

71. What information is required to reset the password?
<--- Score

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

73. Is the team sponsored by a champion or stakeholder leader?

<--- Score

74. Are team charters developed?
<--- Score

75. Has a project plan, Gantt chart, or similar been developed/completed?
<--- Score

76. Is the team equipped with available and reliable resources?
<--- Score

77. When are meeting minutes sent out? Who is on the distribution list?
<--- Score

78. Will vendors be required to implement workflows in business logic?
<--- Score

79. How will variation in the actual durations of each activity be dealt with to ensure that the expected Vulnerability Remediation results are met?
<--- Score

80. How much time will be required from each staff member?
<--- Score

81. Will team members perform Vulnerability Remediation work when assigned and in a timely fashion?
<--- Score

82. Is the Vulnerability Remediation scope

manageable?
<--- Score

83. Do projects specify security testing based on defined security requirements?
<--- Score

84. Do the problem and goal statements meet the SMART criteria (specific, measurable, attainable, relevant, and time-bound)?
<--- Score

85. Does the team have regular meetings?
<--- Score

86. Is there a Vulnerability Remediation management charter, including stakeholder case, problem and goal statements, scope, milestones, roles and responsibilities, communication plan?
<--- Score

87. Is the team adequately staffed with the desired cross-functionality? If not, what additional resources are available to the team?
<--- Score

88. What defines your organizations sphere of influence?
<--- Score

89. Is there a critical path to deliver Vulnerability Remediation results?
<--- Score

90. Is there regularly 100% attendance at the team meetings? If not, have appointed substitutes

attended to preserve cross-functionality and full representation?
<--- Score

91. Are customers identified and high impact areas defined?
<--- Score

92. Are there any constraints known that bear on the ability to perform Vulnerability Remediation work? How is the team addressing them?
<--- Score

93. Do project teams specify requirements based on feedback from other security activities?
<--- Score

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

95. How will the Vulnerability Remediation team and the group measure complete success of Vulnerability Remediation?
<--- Score

96. How do you determine your validation requirements?
<--- 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. What type of analysis is being carried out?
<--- Score

2. Is Process Variation Displayed/Communicated?
<--- Score

3. Which systems would cause the most significant disruption if compromised?
<--- Score

4. Are process variation components displayed/ communicated using suitable charts, graphs, plots?
<--- Score

5. Do project teams specifically analyze design elements for security mechanisms?
<--- Score

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

7. What is the security patch management criteria used to prioritize vulnerability remediation?
<--- Score

8. What is true cyber resilience and to which extent are current measures achieving it?
<--- Score

9. What measures would reduce the vulnerability of elements/groups?
<--- Score

10. Have any major data breach caused your organization to change its mode of operations?
<--- Score

11. How does a given vulnerability impact your own network?
<--- Score

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

13. Which remediation actions should the analyst take to implement a vulnerability management process?
<--- Score

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

15. What are the environmental impacts of your organizations activities?
<--- Score

16. Have you seen your work make an impact?
<--- Score

17. Are vulnerabilities analyzed to determine relevance to your organization?
<--- Score

18. How are the security measures you use deployed?
<--- Score

19. How should vulnerability be measured?
<--- Score

20. How large is the gap between current performance and the customer-specified (goal) performance?
<--- Score

21. What is the scope of the impact?
<--- Score

22. Who participated in the data collection for measurements?

<--- Score

23. Is the component critical per a criticality analysis?
<--- Score

24. How do you evaluate value and impact to the business if compromised?
<--- Score

25. Is the check applied on all the required files and folder within web root directory?
<--- Score

26. Are high impact defects defined and identified in the stakeholder process?
<--- Score

27. Which of the impacted services you need to get to first?
<--- Score

28. What should you measure to track changes over time?
<--- Score

29. What tools and techniques work in malware analysis?
<--- Score

30. Are key measures identified and agreed upon?
<--- Score

31. What are the agreed upon definitions of the high impact areas, defect(s), unit(s), and opportunities that will figure into the process capability metrics?

<--- Score

32. Does a new policy outweigh the cost of all breaches put together?
<--- Score

33. How do you risk prioritize your vulnerability remediation efforts?
<--- Score

34. Which parts will have most impact?
<--- Score

35. Is long term and short term variability accounted for?
<--- Score

36. How does security fit in your priorities?
<--- Score

37. Do you also track/report on root cause as part of your process?
<--- Score

38. Is a solid data collection plan established that includes measurement systems analysis?
<--- Score

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

40. How does software patching impact business operations?
<--- Score

41. Do cybersecurity initiatives receive adequate support and priority?
<--- Score

42. Have you found any 'ground fruit' or 'low-hanging fruit' for immediate remedies to the gap in performance?
<--- Score

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

44. What are the major root causes of security issues?
<--- Score

45. Which performance measures matter most to you?
<--- Score

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

47. Which vulnerabilities should you prioritize for remediation?
<--- Score

48. Are all of the entry points and trust boundaries identified by the design and are in risk analysis report?
<--- Score

49. Is data collection planned and executed?
<--- Score

50. Is key measure data collection planned and executed, process variation displayed and communicated and performance baselined?
<--- Score

51. Are you better equipped to prioritize your vulnerabilities for remediation?
<--- Score

52. What data was collected (past, present, future/ongoing)?
<--- Score

53. How mature are your organizations processes for incident detection and analysis?
<--- Score

54. What are your main priorities when doing development?
<--- Score

55. Does the secure design review process incorporate detailed data level analysis?
<--- Score

56. How have environmental impacts been identified or assessed?
<--- Score

57. Do you prioritize any particular type of updates for any machines?
<--- Score

58. Is data collected on key measures that were identified?

<--- Score

59. What are the key input variables? What are the key process variables? What are the key output variables?
<--- Score

60. What other risks does the security solution cause?
<--- Score

61. What has the team done to assure the stability and accuracy of the measurement process?
<--- Score

62. Are multiple analysis results reported and remediated through a single process?
<--- Score

63. Does the secure design review process incorporate detailed data-level analysis?
<--- Score

64. Can project teams access automated code analysis tools to find security problems?
<--- Score

65. What is the expected impact from a single occurrence of the threat?
<--- Score

66. How do security devices impact cybersecurity?
<--- Score

67. Do your priorities change when a deadline approaches?
<--- Score

68. How should active vulnerability scans be managed for environments sensitive to denial of service impacts?
<--- Score

69. What key measures identified indicate the performance of the stakeholder process?
<--- Score

70. Why measure knowing your summary and anything?
<--- Score

71. What charts has the team used to display the components of variation in the process?
<--- Score

72. How would you characterize your organizations ability to prioritize security vulnerabilities?
<--- Score

73. How important are the applications impacted by the vulnerability?
<--- Score

74. Is there a Performance Baseline?
<--- Score

75. Was a data collection plan established?
<--- Score

76. What particular quality tools did the team find helpful in establishing measurements?
<--- Score

77. Do you prioritize remediation based on threat intelligence?
<--- Score

78. Do you define what data leakage is and what factors can cause data leakage?
<--- 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. Can the data collector identify all connections between the data network in your business?
<--- Score

2. Was a cause-and-effect diagram used to explore the different types of causes (or sources of variation)?
<--- Score

3. Do you have a process for keeping all your software up to date?
<--- Score

4. What constitutes an appropriate verification process for corporate human rights performance?
<--- Score

5. Has the data been assessed as reliable?
<--- Score

6. Does data collector record and document all investigations and findings?
<--- Score

7. How should inputs, functionality, and data be restricted?
<--- Score

8. Were there any improvement opportunities identified from the process analysis?
<--- Score

9. What data types are currently stored by your organization?
<--- Score

10. Are regular compliance checks regarding the collection of personal data and user consent in place?
<--- Score

11. Do governance processes and your organizational culture enable effective cyber risk management?
<--- Score

12. Do you have control about who can see which data returned from your BI tools?

<--- Score

13. Is there any sensitive data in configuration files?
<--- Score

14. Are security checks placed before processing inputs?
<--- Score

15. Does data collector destroy media when it is no longer needed for business or legal reasons?
<--- Score

16. Did any value-added analysis or 'lean thinking' take place to identify some of the gaps shown on the 'as is' process map?
<--- Score

17. How to improve the review process for software components?
<--- Score

18. How mature are your organizations processes for incident handling?
<--- Score

19. Is your documented process aligned with the requirements?
<--- Score

20. What is your exception/escalation process for critical assets, if any?
<--- Score

21. What factors drive remediation performance?

<--- Score

22. How do you secure your data centers and facilities?
<--- Score

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

24. Is code signing routinely performed on software components using a consistent process?
<--- Score

25. Do projects utilize a change management process that is well understood?
<--- Score

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

27. Do you have any selection criteria or process?
<--- Score

28. What quality tools were used to get through the analyze phase?
<--- Score

29. Do any users have only partial access to certain types of system data?
<--- Score

30. Where is the information accessed, processed, and stored?
<--- Score

31. Is the performance gap determined?
<--- Score

32. Was a detailed process map created to amplify critical steps of the 'as is' stakeholder process?
<--- Score

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

34. How much data could be disclosed and how sensitive is it?
<--- Score

35. What drive better/worse remediation performance?
<--- Score

36. How are cti data and information being utilized in your organization?
<--- Score

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

38. What is different about database vulnerability assessment?
<--- Score

39. What does the data say about the performance of the stakeholder process?
<--- Score

40. What is special about the database case?
<--- Score

41. How is cti data and information being utilized in your organization?
<--- Score

42. What did the team gain from developing a sub-process map?
<--- Score

43. Where do you store the metadata?
<--- Score

44. Have the problem and goal statements been updated to reflect the additional knowledge gained from the analyze phase?
<--- Score

45. Is a consistent process used to apply upgrades and patches to critical dependencies?
<--- Score

46. Have data and systems been formally classified based on the business value?
<--- Score

47. What aspects or steps in your update management process work well for you?
<--- Score

48. What are the data collection and reporting considerations?
<--- Score

49. How was the detailed process map generated,

verified, and validated?
<--- Score

50. Do projects follow a consistent process to evaluate and report on security tests to stakeholders?
<--- Score

51. What conclusions were drawn from the team's data collection and analysis? How did the team reach these conclusions?
<--- Score

52. Do you predict trends based on the collected data?
<--- Score

53. Who is involved in the FedRAMP process?
<--- Score

54. Have you evolved your security architecture and associated processes?
<--- Score

55. Are gaps between current performance and the goal performance identified?
<--- Score

56. Were Pareto charts (or similar) used to portray the 'heavy hitters' (or key sources of variation)?
<--- Score

57. What aspects or steps in your update management process are most challenging to handle?
<--- Score

58. Is the gap/opportunity displayed and communicated in financial terms?
<--- Score

59. What factors drive better/worse remediation performance?
<--- Score

60. What are the main advantages of the current software updating process?
<--- Score

61. Who has access to sensitive data – internally and externally?
<--- Score

62. Does the cloud provider have security/data breach protocols?
<--- Score

63. What are the main disadvantages of your current software updating process?
<--- Score

64. Are data backup procedures per the commands back up and recovery instruction?
<--- Score

65. Did the investigator assure of the confidentiality of the data?
<--- Score

66. Is the Vulnerability Remediation process severely broken such that a re-design is necessary?
<--- Score

67. Did any additional data need to be collected?
<--- Score

68. How can it get actionable insights from diverse data?
<--- Score

69. Does data collector require an employees user name and password to be different?
<--- Score

70. Are users restricted to certain functions and data?
<--- Score

71. What are the main advantages of your current software updating process?
<--- Score

72. How to process in multi threaded environment?
<--- Score

73. What tools were used to generate the list of possible causes?
<--- Score

74. Does the cloud provider charge a fee to remove data upon termination of the contract?
<--- Score

75. What are the main disadvantages of the current software updating process?
<--- Score

76. Are it processes designed and operating to detect cyber threats?
<--- Score

77. What are the data backup policies and procedures?
<--- Score

78. What are the revised rough estimates of the financial savings/opportunity for Vulnerability Remediation improvements?
<--- Score

79. Is the data sent on encrypted channel?
<--- Score

80. Does the api access critical data or functions?
<--- Score

81. Does your organization utilize a consistent process for incident reporting and handling?
<--- Score

82. Has your data been exposed – and would you know if it were?
<--- Score

83. What specific vulnerability checks should be present in your database assessment product?
<--- Score

84. What were the crucial 'moments of truth' on the process map?
<--- Score

85. What is the average amount of data you will

lose on an annual basis due to security breaches?
<--- Score

86. Were any designed experiments used to generate additional insight into the data analysis?
<--- Score

87. Are storage of data and investigating products locked?
<--- Score

88. What sensitive data do you have that needs to be protected?
<--- Score

89. How does the process differ depending on who owns the machines, if at all?
<--- Score

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

91. Does data collector have a procedure for customers wishing to file a grievance or complaint?
<--- Score

92. What are the legal means required for a customers survival when data is corrupted or lost?
<--- Score

93. Who is responsible for protecting your sensitive data?
<--- Score

94. Does data collector have a risk assessment process in place?
<--- Score

95. Why does your deployment process differ for different machines?
<--- Score

96. What is the best process for tackling tasks?
<--- Score

97. What tools were used to narrow the list of possible causes?
<--- Score

98. Do you know which processes and/or systems represent the greatest assets from a cybersecurity perspective?
<--- Score

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

100. Are solutions driven by your own or organization policy?
<--- Score

101. What were the financial benefits resulting from any 'ground fruit or low-hanging fruit' (quick fixes)?
<--- Score

102. Who is responsible for the oversight of vendors that may hold sensitive data?
<--- Score

103. Is there any way to express how current the data is?
<--- Score

104. What is the process of the code review when code during the code review needs to be changed?
<--- Score

105. Has your organization established formal governance and controls to protect the sensitive data?
<--- Score

106. Is data and process analysis, root cause analysis and quantifying the gap/opportunity in place?
<--- Score

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

108. Does data collector store sensitive authentication data after authorization?
<--- Score

109. What is the cost of poor quality as supported by the team's analysis?
<--- Score

110. Have any additional benefits been identified that will result from closing all or most of the gaps?
<--- Score

111. Are you vulnerable to data exposure?
<--- 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. Describe the design of the pilot and what tests were conducted, if any?
<--- Score

2. Is penetration testing performed on high risk projects prior to release?
<--- Score

3. What do you need to know to manage risk?
<--- Score

4. What were the underlying assumptions on the cost-benefit analysis?
<--- Score

5. Does the solution provide a unified view of vulnerabilities, configurations, and asset information?
<--- Score

6. Were any criteria developed to assist the team in testing and evaluating potential solutions?
<--- Score

7. Do projects document operational environment security requirements?
<--- Score

8. What tools were used to evaluate the potential solutions?
<--- Score

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

10. Has that assumption been built into the document?
<--- Score

11. How did the team generate the list of possible solutions?
<--- Score

12. Does a minimum security baseline exist for secure design review results?

<--- Score

13. What residual disabling effects are direct results of the amputation?
<--- Score

14. How is leadership engaged and committed to addressing cyber risks facing the business?
<--- Score

15. What types and how many resources do you need to remove risk?
<--- Score

16. Do projects in your organization consider and document likely threats?
<--- Score

17. Are improved process ('should be') maps modified based on pilot data and analysis?
<--- Score

18. Is the optimal solution selected based on testing and analysis?
<--- Score

19. Do you have at least one security savvy programmer on every critical development project?
<--- Score

20. How do you see a cyber threat developing?
<--- Score

21. What error proofing will be done to address some of the discrepancies observed in the 'as is' process?

<--- Score

22. Are security related alerts and error conditions documented on a per project basis?
<--- Score

23. Should you seriously consider an open source solution?
<--- Score

24. Are developers tested to ensure a baseline skill set for secure development practices?
<--- Score

25. Does a minimum security baseline exist for code review results?
<--- Score

26. Are there clearly defined criteria for remediation of security risk for products in development?
<--- Score

27. How much time on average does your development team spend remediating each vulnerability found in development?
<--- Score

28. How will the group know that the solution worked?
<--- Score

29. Is a solution implementation plan established, including schedule/work breakdown structure, resources, risk management plan, cost/budget, and control plan?

<--- Score

30. How will you reduce the risk of similar vulnerabilities getting into your code base in the future?
<--- Score

31. Can the application revert back to normal operation when the security risk score drops to normal levels?
<--- Score

32. Does the solutions architecture provide flexibility to tune scanning configuration for optimal performance?
<--- Score

33. What percentage of remediated vulnerabilities are actually high risk?
<--- Score

34. Are new and improved process ('should be') maps developed?
<--- Score

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

36. Does the solution perform configuration and compliance assessments in a single scan with unified reporting?
<--- Score

37. Do project teams specify security requirements during development?
<--- Score

38. Do project teams specifically consider risk from external software?
<--- Score

39. Does the solution provide an approval work flow for vulnerability exceptions?
<--- Score

40. What is Vulnerability Remediation's impact on utilizing the best solution(s)?
<--- Score

41. Do project teams review selected high risk code?
<--- Score

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

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

44. How big are cyber risks for your organization and your organizations you do business with?
<--- Score

45. How will the team or the process owner(s) monitor the implementation plan to see that it is working as intended?
<--- Score

46. How do you get control over development?
<--- Score

47. Do you use any technical solutions to protect users?
<--- Score

48. Do stakeholders consistently review results from code reviews?
<--- Score

49. Does your organization know about what is required based on risk ratings?
<--- Score

50. Does your organization evaluate your own suppliers on environmental issues?
<--- Score

51. What kind of software development model do you use?
<--- Score

52. Has your organization ever been breached as a result of a vulnerability being left unpatched?
<--- Score

53. Which percentage of overall vulnerabilities are high risk?
<--- Score

54. When are the results of the further assessment expected to be available?
<--- Score

55. Is pilot data collected and analyzed?
<--- Score

56. How do you incentivize industry to design,

implement, maintain effective cybersecurity solutions?
<--- Score

57. How to identify and mitigate cybersecurity risks across multiple public and private organizations?
<--- Score

58. What controls are needed to satisfy the security requirements to mitigate risk?
<--- Score

59. What are application security risks?
<--- Score

60. Are the best solutions selected?
<--- Score

61. How does dialogue relate to human rights and sustainable development in a democratic context?
<--- Score

62. Has the quality of supplied products improved?
<--- Score

63. How are administrators alerted when security risk score rises?
<--- Score

64. What else are you going to do that will improve the result next time?
<--- Score

65. How should a developer or project manager

choose?
<--- Score

66. Can the solution integrate with private and public container registries to assess images?
<--- Score

67. How do you aggregate assessment results?
<--- Score

68. How much time on average does your development team spend remediating each vulnerability found in production?
<--- Score

69. What type of development do you do?
<--- Score

70. What is the implementation plan?
<--- Score

71. How does the solution remove the key sources of issues discovered in the analyze phase?
<--- Score

72. What percentage of exploited or high risk vulnerabilities were actually remediated?
<--- Score

73. What observable behavior might put your enterprise at risk?
<--- Score

74. Does your organization periodically assess risk using the criteria set forth in the control requirement?

<--- Score

75. What tools were used to tap into the creativity and encourage 'outside the box' thinking?
<--- Score

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

77. What communications are necessary to support the implementation of the solution?
<--- Score

78. Is there a small-scale pilot for proposed improvement(s)? What conclusions were drawn from the outcomes of a pilot?
<--- Score

79. Can the solution perform discovery, vulnerability, and configuration assessments in a single unified scan?
<--- Score

80. What should a solutions architect do to remediate the vulnerability?
<--- Score

81. What tools were most useful during the improve phase?
<--- Score

82. Was a pilot designed for the proposed solution(s)?
<--- Score

83. Where and how much do you need to invest to

optimize your cyber capabilities?
<--- Score

84. Does each project team understand where to find secure development best practices and guidance?
<--- Score

85. What lessons, if any, from a pilot were incorporated into the design of the full-scale solution?
<--- Score

86. Is there a cost/benefit analysis of optimal solution(s)?
<--- Score

87. Which percentage of overall vulnerabilities are high risks?
<--- Score

88. Does your solution provide auditing, reporting, and alerting for security related events and information?
<--- Score

89. Do you evaluate the effectiveness of cybersecurity?
<--- Score

90. Is software assurance considered in all phases of development?
<--- Score

91. What percentage of exploited or high risk vulnerabilities are remediated?
<--- Score

92. Do projects use automation to evaluate security test cases?
<--- Score

93. Are possible solutions generated and tested?
<--- Score

94. What level of solution, workaround, or other remediation is available?
<--- Score

95. Are there any constraints (technical, political, cultural, or otherwise) that would inhibit certain solutions?
<--- Score

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

97. How intense is the pain associated with the arthritis, is it so intense that it results in loss of work time?
<--- Score

98. Do project teams document the attack perimeter of software designs?
<--- Score

99. How will cybersecurity risk be assessed and management during the lifecycle?
<--- Score

100. How is absolute reach different from existing

scripting solutions?
<--- Score

101. Do you really need to understand the fundamentals of security in order to protect your network?
<--- Score

102. What is the team's contingency plan for potential problems occurring in implementation?
<--- Score

103. What do you do to reduce your risk?
<--- Score

104. What level of testing should be done to develop baselines?
<--- Score

105. What areas are most crucial for risk reduction within your business?
<--- Score

106. How do you balance technology risks and rewards?
<--- Score

107. What does the 'should be' process map/design look like?
<--- Score

108. Are you seeing your results in real time?
<--- Score

109. What improvements have been made as a result of the policy?

<--- Score

110. Who owns the responsibility to remediate the vulnerability of a solution, SaaS infrastructure or corporate system?
<--- Score

111. Does your organization understand and document the types of attackers it faces?
<--- Score

112. Is cybersecurity your organization risk management issue?
<--- Score

113. Has a security risk assessment and architectural review been performed?
<--- Score

114. What attendant changes will need to be made to ensure that the solution is successful?
<--- Score

115. Is the board demonstrating due diligence, ownership, and effective management of information risk?
<--- Score

116. Do the business stakeholders understand your organizations risk profile?
<--- Score

117. Is the implementation plan designed?
<--- Score

118. Are risk ratings used to tailor the required

assurance activities?
<--- Score

119. Is a contingency plan established?
<--- 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. Do project teams check software designs against known security risks?
<--- Score

2. Have new or revised work instructions resulted?
<--- Score

3. What is the control/monitoring plan?
<--- Score

4. Is the purpose of the plans engagement to inform stakeholders?
<--- Score

5. Which engagement techniques will you use in the engagement plan?
<--- Score

6. Have you designed an evaluation process as part of your engagement plan?
<--- Score

7. Who is responsible for planning and implementing flaw remediation security controls?
<--- Score

8. Who is responsible for assessing, and monitoring flaw remediation security controls?
<--- Score

9. Are developers provided with test results and remediation plans?
<--- Score

10. What is the recommended frequency of auditing?
<--- Score

11. How does the solution monitor remote users and endpoints that disconnect from the network?
<--- Score

12. When a cybersecurity incident occurs, what is your plan of response?
<--- Score

13. Is there a transfer of ownership and knowledge

to process owner and process team tasked with the responsibilities.
<--- Score

14. How do other organizations plan to improve the vulnerability risk management program next year?
<--- Score

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

16. Who is the Vulnerability Remediation process owner?
<--- Score

17. Is the purpose of the plans engagement to consult stakeholders?
<--- Score

18. How are you anticipating and adapting your strategy and controls?
<--- Score

19. Are you enhancing and aligning your plan to ongoing business changes?
<--- Score

20. What are the critical security controls?
<--- Score

21. What is the impact of the plan to business operations?
<--- Score

22. Are production standards reviewed periodically?
<--- Score

23. Do penetration tests result in remediation plans?
<--- Score

24. What other areas of the group might benefit from the Vulnerability Remediation team's improvements, knowledge, and learning?
<--- Score

25. Is there a need to tailor infosec standards to certain types of information, and if so how?
<--- Score

26. Has the improved process and its steps been standardized?
<--- Score

27. Is the approver available to review and accept the plan?
<--- Score

28. Does the plan consider how the contaminant type might affect the extent of engagement?
<--- Score

29. How might the group capture best practices and lessons learned so as to leverage improvements?
<--- Score

30. Is there a recommended audit plan for routine surveillance inspections of Vulnerability Remediation's gains?

<--- Score

31. Are suggested corrective/restorative actions indicated on the response plan for known causes to problems that might surface?
<--- Score

32. Does the plan consider how the engagement techniques will be delivered?
<--- Score

33. Is there a standardized process?
<--- Score

34. How will the day-to-day responsibilities for monitoring and continual improvement be transferred from the improvement team to the process owner?
<--- Score

35. Is knowledge gained on process shared and institutionalized?
<--- Score

36. Are you aware of any information security standards that your organization has?
<--- Score

37. Is reporting being used or needed?
<--- Score

38. Is the purpose of the plans engagement activities to involve stakeholders?
<--- Score

39. What quality tools were useful in the control

phase?
<--- Score

40. Do you have a plan to react to an attack and minimize the harm caused?
<--- Score

41. What other systems, operations, processes, and infrastructures (hiring practices, staffing, training, incentives/rewards, metrics/dashboards/scorecards, etc.) need updates, additions, changes, or deletions in order to facilitate knowledge transfer and improvements?
<--- Score

42. Are documented procedures clear and easy to follow for the operators?
<--- Score

43. Are projects periodically audited to ensure a baseline of compliance with policies and standards?
<--- Score

44. What type of online engagement will the plan use?
<--- Score

45. What is the difference between FISMA and FedRAMP controls?
<--- Score

46. Are the plan, test results, and flaw remediation results documented?
<--- Score

47. Does your organization systematically use audits to collect and control compliance evidence?
<--- Score

48. Does the plan acknowledge the role that local organizations can play in representing local communities?
<--- Score

49. Which vulnerabilities must one remediate in order to have a clean scan under PCI DSS standards?
<--- Score

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

51. How to standardize sla for data recovery vulnerability?
<--- Score

52. Is there documentation that will support the successful operation of the improvement?
<--- Score

53. Is a response plan established and deployed?
<--- Score

54. What are the critical parameters to watch?
<--- Score

55. What is your plan for distributing contracts to your employees?
<--- Score

56. How has the program planning change recently?
<--- Score

57. Do project teams utilize automation to check code against application specific coding standards?
<--- Score

58. Is there a test plan in place and are tools available to perform security testing?
<--- Score

59. Are new process steps, standards, and documentation ingrained into normal operations?
<--- Score

60. How will the process owner and team be able to hold the gains?
<--- Score

61. Does the cloud provider have a standard contract/terms of service or is it negotiated?
<--- Score

62. Is the purpose of the plans engagement to collaborate with stakeholders?
<--- Score

63. Are operating procedures consistent?
<--- Score

64. Does the Vulnerability Remediation performance meet the customer's requirements?
<--- Score

65. Does the engagement plan include a description of it management plan?
<--- Score

66. Does job training on the documented procedures need to be part of the process team's education and training?
<--- Score

67. Is new knowledge gained imbedded in the response plan?
<--- Score

68. What should the next improvement project be that is related to Vulnerability Remediation?
<--- Score

69. Is the purpose of the plans engagement to empower stakeholders?
<--- Score

70. Have your business leaders undertaken cyberattack scenario planning?
<--- Score

71. How will new or emerging customer needs/ requirements be checked/communicated to orient the process toward meeting the new specifications and continually reducing variation?
<--- Score

72. Is your main financial planning system and its supporting infrastructure vulnerable to manipulation?
<--- Score

73. Is a response plan in place for when the input, process, or output measures indicate an 'out-of-control' condition?
<--- Score

74. Does a troubleshooting guide exist or is it needed?
<--- Score

75. Have the security controls been implemented or is there a plan in place?
<--- Score

76. How will the process owner verify improvement in present and future sigma levels, process capabilities?
<--- Score

77. How will input, process, and output variables be checked to detect for sub-optimal conditions?
<--- Score

78. Does your organization have a standard desktop configuration and software standards?
<--- Score

79. Is there a maintenance and/or technical hotline support services plan?
<--- Score

80. Are the majority of the protection mechanisms and controls captured and mapped back to threats?
<--- Score

81. What plans do you have to ensure staffing capacity?
<--- Score

82. Is there a control plan in place for sustaining improvements (short and long-term)?
<--- Score

83. Who is responsible for authorizing flaw remediation security controls?
<--- Score

84. Does the response plan contain a definite closed loop continual improvement scheme (e.g., plan-do-check-act)?
<--- Score

85. Does the design implement access control for all resources?
<--- Score

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

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

88. Is there a documented and implemented monitoring plan?
<--- Score

89. Are the controls and safeguards periodically tested?
<--- Score

90. Do project teams build software from centrally controlled platforms and frameworks?

<--- Score

91. Are project teams able to request an audit for compliance with policies and standards?
<--- Score

92. Does the plan consider the need for reporting, updating and ongoing evaluation?
<--- Score

93. Do stakeholders review access control matrices for relevant projects?
<--- Score

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

95. What are your plans for collecting, refreshing, and distributing devices to employees?
<--- Score

96. Are development staff aware of future plans for the assurance program?
<--- Score

97. Are all the engagement activities detailed in the plan necessary?
<--- Score

98. What key inputs and outputs are being measured on an ongoing basis?
<--- Score

99. Did you conduct a needs assessment of your stakeholders to include needs in your planning?

<--- Score

100. What are the stakeholder engagement plans sections and supporting principles?
<--- Score

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

102. Which compliance standards must be met?
<--- Score

103. How will report readings be checked to effectively monitor performance?
<--- Score

104. What security mechanisms/controls are you having trouble implementing?
<--- Score

105. Does your organization utilize a set of policies and standards to control software development?
<--- Score

106. Are there documented procedures?
<--- Score

107. Will any special training be provided for results interpretation?
<--- Score

108. What security measurement practices and data does your organization use to assist product planning?
<--- 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 #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. How should the team work together?
<--- Score

2. How is the information actually shared securely?
<--- Score

3. Are you sure your cloud environments are really safe?
<--- Score

4. Do you ever seek additional information about updates?
<--- Score

5. What are the most important things to consider to secure the network?
<--- Score

6. What is the total population of your organization?
<--- Score

7. Is the team running scripts to check for compliance when code is checked in?
<--- Score

8. What information is deemed critical and why?
<--- Score

9. How do you manage application security?
<--- Score

10. Is a vulnerability assessment program expensive?
<--- Score

11. What is different in conflict affected areas?
<--- Score

12. Are weak crypto keys generated, or is proper key management or rotation missing?
<--- Score

13. What is the industry of your organization that you work for?
<--- Score

14. How do you specify what kind of response information could be accepted?

<--- Score

15. What facility entry and exit protocols will be established for employees and visitors?
<--- Score

16. Which security activity is most effective in finding vulnerabilities?
<--- Score

17. How does your program compare to CMM?
<--- Score

18. Is anybody already at the edge of information overload?
<--- Score

19. When should companies provide for remediation?
<--- Score

20. Which environmental actions has your organization introduced or supported within the last year, if any?
<--- Score

21. Do the logs contain sensitive information?
<--- Score

22. Does software have a positive reputation?
<--- Score

23. How are other organizations performing in reality?
<--- Score

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

25. Do roles or responsibilities change for each project?
<--- Score

26. Does your organization have an assigned security response team?
<--- Score

27. How certain is the information included in the record?
<--- Score

28. Has your organization kept pace?
<--- Score

29. Is any further assessment being undertaken?
<--- Score

30. Should you differentiate between internal & external systems?
<--- Score

31. What is web application security testing?
<--- Score

32. Are vulnerabilities being exploited in the wild?
<--- Score

33. Are project stakeholders aware of how to obtain a formal secure design review?
<--- Score

34. How do departments outpace cyber threats?
<--- Score

35. Are security notes delivered with each software release?
<--- Score

36. Can the pedigree of the software be established?
<--- Score

37. Has new technology been introduced to your organization?
<--- Score

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

39. What would help you to better manage software updates for multiple machines?
<--- Score

40. How do you know when remediation is complete and verified?
<--- Score

41. Are security patches smaller than non security bug fixes?
<--- Score

42. Where are you suggesting putting that information?
<--- Score

43. Where are the application properties/ configuration parameters stored?

<--- Score

44. What does application containment do?
<--- Score

45. Does your organization have any security related policies for machines?
<--- Score

46. How much influence does your organization have?
<--- Score

47. Are your systems really protected?
<--- Score

48. What information is important to track?
<--- Score

49. Do you believe your vulnerability remediation program is mature?
<--- Score

50. How do you check if the product is ready for distribution?
<--- Score

51. Does your organization have a vulnerability management program?
<--- Score

52. How do you timely and efficiently determine when to take action?
<--- Score

53. Do project stakeholders know the projects

compliance status?
<--- Score

54. What organizations and departments work with older people?
<--- Score

55. Are your top people leaving you and your organization?
<--- Score

56. Are the stakeholders aware of the location of the contamination?
<--- Score

57. Where are the gaps in your programmers secure coding knowledge and skills?
<--- Score

58. Is there to be an allowance made for re testing for the system after remediation?
<--- Score

59. Are employees practicing self awareness?
<--- Score

60. How frequently are vulnerabilities unpatched when disclosed?
<--- Score

61. What is the actual severity of the vulnerability?
<--- Score

62. Is the median lifetime of vulnerabilities decreasing in newer versions?
<--- Score

63. Is information stored on the client that should be stored on the server?
<--- Score

64. Does your organization have any policies on software updates for machines?
<--- Score

65. How often do you see open source vulnerabilities in your ecosystem?
<--- Score

66. Do you advertise shared security services with guidance for project teams?
<--- Score

67. Who is responsible for remediating vulnerabilities?
<--- Score

68. What information is available on the software; in particular, is source code available?
<--- Score

69. Are you reliably addressing your key vulnerabilities?
<--- Score

70. Does the configuration get applied to all files and users?
<--- Score

71. What categories of information assets are included in your vulnerability assessment and remediation program?

<--- Score

72. How long is long enough to respond to a vulnerability?
<--- Score

73. What systems and networks are allowed to be tested?
<--- Score

74. Can an administrator or other user provision accounts with privileges greater than own?
<--- Score

75. What is the goal or objective of the testing team?
<--- Score

76. What is the difference between a code of ethics and a code of conduct?
<--- Score

77. What engagement techniques will be used to collaborate with stakeholders?
<--- Score

78. What information should be provided about the vulnerability?
<--- Score

79. Will vendors be consistent across product lines in terms of how updates are specified?
<--- Score

80. What is the role of the program office?
<--- Score

81. Why is cybersecurity so important?
<--- Score

82. Has the severity of discovered vulnerabilities changed over time?
<--- Score

83. Are sending software instances shared or dedicated?
<--- Score

84. What is the role of software supplied by the vendor?
<--- Score

85. Are your people clear of roles and responsibilities during a cyber crisis?
<--- Score

86. How did you establish the open source program office?
<--- Score

87. Are stakeholders aware of the security test status prior to release?
<--- Score

88. What is the main purpose of your organization you work for?
<--- Score

89. Is your organization routinely targeted and face attempts of attack?
<--- Score

90. What it systems do you have in your enterprise?
<--- Score

91. Does wcps expect the selected vendor to implement remediation activities?
<--- Score

92. What information will you disclose?
<--- Score

93. Are defects and weaknesses tracked from discovery and notification through to remediation?
<--- Score

94. How to build a compliance communication within your organization?
<--- Score

95. Does the application or API detect the attack?
<--- Score

96. Have you performed the proper security hardening across the entire application stack?
<--- Score

97. Is the function going to be available to non authenticated users?
<--- Score

98. Does the code change modify the attack surface?
<--- Score

99. Is password disclosed to user/written to a file/

logs/console?
<--- Score

100. Is it externally facing or internal to trusted users?
<--- Score

101. Who is responsible for running network scans?
<--- Score

102. Why are you spending so much on security vulnerability remediation?
<--- Score

103. How long has the software source been available?
<--- Score

104. What is the configuration, health, or operating system status?
<--- Score

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

106. Are security features correct and is functional code secure?
<--- Score

107. Do you feel your organization can take on additional responsibilities in vulnerability management?
<--- Score

108. What types of vulnerabilities are associated with web resources?
<--- Score

109. Do you rely solely on phishing to ensure your employees are secure?
<--- Score

110. Are you vulnerable to forced access?
<--- Score

111. Is there a software security assurance program in place?
<--- Score

112. Has your organization had to make investment in IT hardware and/or software?
<--- Score

113. How long do vulnerabilities live in code bases?
<--- Score

114. What are the main advantages of the current update information?
<--- Score

115. Do you have one million dollars to spend on application security?
<--- Score

116. Are server side checks done that solely rely on information provided by the attacker?
<--- Score

117. How many employees did your organization

hire?
<--- Score

118. Does your product include scanning functionality, or do you build upon another vendors scanning technology?
<--- Score

119. Will you distribute contracts to all employee groups at the same time?
<--- Score

120. What should the team report, and to whom?
<--- Score

121. How frequently are vulnerabilities fixed by disclosure time?
<--- Score

122. What is it about human behavior that makes cybersecurity so inherently difficult?
<--- Score

123. How many times have the grievance procedures been used during the last year?
<--- Score

124. What are the biggest barriers to remediating and mitigating cybersecurity incidents?
<--- Score

125. What are the top used cloud apps?
<--- Score

126. Is the drawing of the commands network topology current?

<--- Score

127. Do you employ enterprise level desktop configuration management?
<--- Score

128. What are the agents or scripts executing on servers of hosted applications?
<--- Score

129. Who are the users that you manage machines for?
<--- Score

130. What engagement techniques will be used to inform stakeholders?
<--- Score

131. What kind of security regulatory compliance do you meet?
<--- Score

132. What is a fourth of your organizations capitalization?
<--- Score

133. Do you expect the chosen provider to perform remediation for discovered vulnerabilities?
<--- Score

134. Can cybersecurity awareness be trained?
<--- Score

135. What is your organizational structure for sharing information?

<--- Score

136. Is that exception always a user or does it have structure?
<--- Score

137. What weaknesses in your software could be exploited?
<--- Score

138. Do security patches change code base sizes less than non security bug fixes?
<--- Score

139. How much exposure does non compliance introduce?
<--- Score

140. How often are you briefed on your cyber initiatives?
<--- Score

141. Is it the responsibility of your organization itself or the IT supplier to implement and inform of critical security updates?
<--- Score

142. Do you feel vulnerability management is important for your organization like yours?
<--- Score

143. Are you a budding programmer who wants to create the next big app?
<--- Score

144. Does your system have the ability to do

throttling/rate limiting by IP to a specific ISP?
<--- Score

145. What can an unauthenticated user do?
<--- Score

146. Are the networks scanned regularly?
<--- Score

147. Will the application give access to the project?
<--- Score

148. Is your cybersecurity program aligned with your business strategy?
<--- Score

149. Does the system track how many failed login attempts a user has experienced?
<--- Score

150. How are vulnerable items and vulnerability groups assigned to remediation teams?
<--- Score

151. What is the predominant operating system, if any?
<--- Score

152. When did you find the vulnerability?
<--- Score

153. Does your organization or systems requiring remediation face numerous and/or significant threats?
<--- Score

154. Has remediation of all known weaknesses been performed in a timely manner on each of your organizations systems?
<--- Score

155. Can an attacker completely take over and manipulate the system?
<--- Score

156. What is vulnerability scanning and how can it be leveraged?
<--- Score

157. What updates are least important to your organization?
<--- Score

158. How did you assign roles and responsibilities to your employees?
<--- Score

159. Does your vulnerability scanner perform authenticated scans?
<--- Score

160. What is a time when you leveraged pen tests to stop a threat?
<--- Score

161. Does the nature of the vulnerability make it difficult to exploit?
<--- Score

162. How much could be lost if the module has a vulnerability introduced?
<--- Score

163. What exactly are you able to make the application do?
<--- Score

164. What is virtual patching, and how does it work?
<--- Score

165. Is time the only factor at work here?
<--- Score

166. Which vulnerabilities represent the greatest threats?
<--- Score

167. Why do programmers make security errors?
<--- Score

168. What tools are going to be used?
<--- Score

169. How much time do you spend working with other teams on vulnerability remediation, from scan to fix?
<--- Score

170. Do security patches affect fewer source code files than non security bug fixes?
<--- Score

171. When should a vulnerability assessment be used?
<--- Score

172. Is it possible to access that resource after the

log out?
<--- Score

173. Are you spending your time and money in the right areas?
<--- Score

174. Can the common vulnerability scoring system be trusted?
<--- Score

175. What is been the highlight of the program for you?
<--- Score

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

177. What updates are most important to your organization and why?
<--- Score

178. What organizations and departments work with young people?
<--- Score

179. Does organization project estimation allot time for code reviews?
<--- Score

180. Is the test to be performed on a routed network or a local segment?
<--- Score

181. What is the impetus behind information

sharing?
<--- Score

182. Do you keep a log file of any system changes and updates?
<--- Score

183. What are the policies and procedures used to protect sensitive information from unauthorized access?
<--- Score

184. Is the vulnerability actually being exploited?
<--- Score

185. Can the attacker obtain access to sensitive information as secrets, PII?
<--- Score

186. Does your organization regularly compare your security spend with that of other organizations?
<--- Score

187. What is your organization trying to achieve with information security/privacy program?
<--- Score

188. What does crowdsourced security look like?
<--- Score

189. What type of tests do you use to detect security faults in a network and why?
<--- Score

190. What self reporting expectations can be set

forth for self disclosure by employees?
<--- Score

191. Should you be applying red flag thinking to compliance work?
<--- Score

192. How are reset passwords communicated to the user?
<--- Score

193. How long does it take to remediate security defects by type?
<--- Score

194. Is your organizations vulnerability management program winning?
<--- Score

195. Has your organization acquired any other organizations?
<--- Score

196. Will it fit with the culture of your own organization?
<--- Score

197. Is the departure time convenient?
<--- Score

198. Do you have more testing coverage across your attack surface?
<--- Score

199. How long does it take to fix vulnerabilities?
<--- Score

200. What is involved with your recently announced reorganization?
<--- Score

201. How long does it take to detect a cyber attack?
<--- Score

202. Do you use any specific software tool?
<--- Score

203. Can highly subcontracted business models be sustainable?
<--- Score

204. What kind of security do you provide for your emails?
<--- Score

205. What do you do to speed that project up?
<--- Score

206. When do you apply non security related updates?
<--- Score

207. What domains or URLs are associated with delivering exploits for a vulnerability?
<--- Score

208. What can an authenticated user do?
<--- Score

209. What are the threats associated with the security holes, as well as to your business?

<--- Score

210. Why crowdsourced security testing?
<--- Score

211. Will the application know if its being attacked?
<--- Score

212. How closely do other organizations track to the average?
<--- Score

213. Who is behind the clickety clack of the keyboard breaking into your system?
<--- Score

214. Do project stakeholders know projects compliance status?
<--- Score

215. Does migrating a monolithic system to microservices decrease the technical debt?
<--- Score

216. What role does security play in a network?
<--- Score

217. What is a cyber readiness assessment?
<--- Score

218. How does a workforce introduce the security skills to implement a secure code review methodology?
<--- Score

219. What is the lowest wage paid by you to an employee on a full time basis?
<--- Score

220. Is any of your software out of date?
<--- Score

221. Have new facilities been added or removed from your organization?
<--- Score

222. What engagement techniques will be used to involve stakeholders?
<--- Score

223. Is your crowdsourced security testing successful?
<--- Score

224. Are any compiler warnings disabled in code being delivered?
<--- Score

225. How are you securing new technology adoption and managing vulnerability with your legacy technology?
<--- Score

226. How large is your organization that you work for?
<--- Score

227. Where is your secret access key?
<--- Score

228. What malicious files are known to exploit a

vulnerability?
<--- Score

229. Do you know what information is most valuable to the business?
<--- Score

230. Are there still security holes lurking in your system?
<--- Score

231. Does your policy include mergers and acquisition terms?
<--- Score

232. What are the best practices for getting started with open source governance for software companies?
<--- Score

233. Is the program designed to fail gracefully?
<--- Score

234. Are all your employees working in your organization of own free will?
<--- Score

235. Are project teams audited for the use of secure architecture components?
<--- Score

236. How secure is the code on your side?
<--- Score

237. Do session ids timeout and can users log out?
<--- Score

238. Does application use custom schemes for hashing and or cryptographic?
<--- Score

239. How numerous are security flaws compared to security bugs?
<--- Score

240. How did you decide to use open source components or codes in your product or service?
<--- Score

241. Is the first character of the users password a?
<--- Score

242. How do you inform affected parties about vulnerabilities on large scale?
<--- Score

243. Are you and your organization ready to deal with a cyber crisis?
<--- Score

244. Who leads your incident and crisis management program?
<--- Score

245. Are all flaw remediation updates tracked as part of the systems configuration baseline?
<--- Score

246. How do you configure your systems more securely?
<--- Score

247. Why is application security important?
<--- Score

248. How are security vulnerabilities discovered?
<--- Score

249. What will you do differently next time?
<--- Score

250. How does rollback remediation work?
<--- Score

251. What program tools will be used?
<--- Score

252. What is it concerning networking and services?
<--- Score

253. Why sell yourself short and swear that only one vendor has the best product?
<--- Score

254. Why sunbelt network security inspector?
<--- Score

255. Is the code reviewer knowledgeable about the domain knowledge of the code that is being reviewed?
<--- Score

256. How much insight and intelligence do you hope to capture from your program?
<--- Score

257. Has the bureau given any thought to

cybersecurity, as well as physical security?
<--- Score

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

259. Are vulnerability patches publicly visible long before disclosure?
<--- Score

260. What is the status of the project which you have just indicated was funded?
<--- Score

261. Does your error handling reveal stack traces or other overly informative error messages to users?
<--- Score

262. Is your organization response team ready?
<--- Score

263. How well protected is the information to unauthorized access?
<--- Score

264. Who in your organization is responsible for vulnerability management?
<--- Score

265. Does the vulnerability affect systems within your organizations network?
<--- Score

266. Are you reviewing for security, functionality,

maintainability, and/or style?
<--- Score

267. Who has access to your organizations most valuable information?
<--- Score

268. What updates are most important to your organization?
<--- Score

269. Are stakeholders aware of relevant threats and ratings?
<--- Score

270. Which main environmental targets has your organization worked towards during the last year?
<--- Score

271. How do you know if the CISOs security program has accounted for all the components to be effective?
<--- Score

272. How have your business practices evolved to address the threats to your business?
<--- Score

273. Are project releases audited for appropriate operational security information?
<--- Score

274. Is it the only method that will work?
<--- Score

275. Who is the users of the application?

<--- Score

276. What does success look like for your organization?
<--- Score

277. How do you ensure that all employees and staff are treated equitably?
<--- Score

278. How did you find the vulnerability?
<--- Score

279. Do you guess how many times your organization has been hacked?
<--- Score

280. What exactly is vulnerability assessment, and how does it differ from penetration testing?
<--- Score

281. Does the application contain any business sensitive information?
<--- Score

282. How many days off would a full time production worker or the like have in an average week?
<--- Score

283. Are there any obligations by your supervisor/ employer for performing security testing?
<--- Score

284. Are vulnerability scores used consistently?
<--- Score

285. Who on your team is responsible for privacy?
<--- Score

286. Are the applications running on the endpoint critical for your organization?
<--- Score

287. Is the code being integrated into the project fully vetted by IT management and approved?
<--- Score

288. Is it possible to break into the secure network between you?
<--- Score

289. What are the operating systems on the machines that you manage?
<--- Score

290. Are vulnerabilities reduced to an acceptable level for release?
<--- Score

291. How easy or difficult is it to exploit weaknesses?
<--- Score

292. Do you have an insider threat program?
<--- Score

293. Do security and non security bug fixes always modify source code?
<--- Score

294. Does your ics vendor respond to

vulnerabilities that are provided to it?
<--- Score

295. Did it involve performing some form of vulnerability scanning?
<--- Score

296. Why would you want anything less for the security of your networks and systems?
<--- Score

297. Does your infrastructure support dedicated IPs for each business unit for sending?
<--- Score

298. Is the vulnerability pertinent to your organizations operations?
<--- Score

299. Do you disseminate patch update information throughout organizations local systems administrators?
<--- Score

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

301. What is cyber incident simulation?
<--- Score

302. Is it subject to a current site contamination audit?
<--- Score

303. Is there a capability maturity model for threat

and vulnerability management?
<--- Score

304. How do you remediate the vulnerability?
<--- Score

305. Which of your programmers and contractors have the strongest secure coding skills?
<--- Score

306. What type of information do you consider to be part of your intelligence gathering?
<--- Score

307. Does a minimum security baseline exist for security testing?
<--- Score

308. Is there a preference between commercial or free tools?
<--- Score

309. What policy levers do you have for reducing vulnerability?
<--- Score

310. Do you see a reduction in vulnerabilities introduced into your digital environment?
<--- Score

311. How easy is it to reproduce an attack to work?
<--- Score

312. What would your ideal way to handle software updates be?
<--- Score

313. How do you track how well updates have been installed on different machines?
<--- Score

314. Which is your vulnerability scanner configured to scan?
<--- Score

315. Does your organization perform vulnerability scanning?
<--- Score

316. Are there unused configurations related to business logic?
<--- Score

317. Does your organization have an environmental management system or programme?
<--- Score

318. What type of updates do you install regularly?
<--- Score

319. Which team is more productive in fixing security defects and vulnerabilities?
<--- Score

320. What attacks can exploit which weaknesses?
<--- Score

321. What procedures do you have for keeping employees personal information confidential?
<--- Score

322. What is your organizations involvement in vulnerability management?
<--- Score

323. Are there any sanctions for inaccurate or incomplete or untimely reporting?
<--- Score

324. Does the tool support the programming language used?
<--- Score

325. Is it a server side web application, embedded, or something else?
<--- Score

326. Do you make a backup of your system before applying patches?
<--- Score

327. What happens when vulnerabilities are discovered?
<--- Score

328. Can an attacker crash the system?
<--- Score

329. Which of your products include software?
<--- Score

330. Do you properly use iDefence tools?
<--- Score

331. What are the approximate number of users using the application?
<--- Score

332. When do you apply security updates?
<--- Score

333. How does the application maintain security?
<--- Score

334. How are human rights relevant to business?
<--- Score

335. Do project teams use a method of rating threats for relative comparison?
<--- Score

336. Are user inputs used to directly reference business logic?
<--- Score

337. Do security patches make fewer logical changes than non security bug fixes?
<--- Score

338. Are you safe from malicious code?
<--- Score

339. Are vulnerability reporting rates declining?
<--- Score

340. What are the areas where the trend is going up and how to normalize areas?
<--- Score

341. How can technologists become forces for the public interest within own organizations?
<--- Score

342. Are licensed software components still valid for the intended use?
<--- Score

343. Can the infrastructure and communication network be trusted?
<--- Score

344. What will you do in the same way next time?
<--- Score

345. Are vulnerability tests conducted on a quarterly basis?
<--- Score

346. Are any old or weak cryptographic algorithms used either by default or in older code?
<--- Score

347. Can an administrator provision other administrators or just users?
<--- Score

348. What kind of business model do you have?
<--- Score

349. What type of machines/devices do you manage?
<--- Score

350. How to ensure license compliance for outgoing products?
<--- Score

351. What engagement techniques will be used to consult stakeholders?

<--- Score

352. Is your organization experiencing compliance fatigue?
<--- Score

353. Is the internal network secure from unauthorized electronic access?
<--- Score

354. Can decentralization be implemented to address the particular type of singularity?
<--- Score

355. Are some resources more important that others, therefore requiring higher security?
<--- Score

356. Do you feel your organization devotes the adequate amount of resources to vulnerability management?
<--- Score

357. Is your organization environment getting complex day by day?
<--- Score

358. Is targeting deprived areas an effective means to reach poor people?
<--- Score

359. Why have so few vulnerabilities been reported that were introduced in later versions?
<--- Score

360. Do you already have IS security hygiene

guidelines?
<--- Score

361. Will your organization work to secure an agreement?
<--- Score

362. What information is being shared, and what is the purpose of sharing it?
<--- Score

363. Do you ensure compliance with local environmental regulation?
<--- Score

364. Does the product interoperate with other security technologies?
<--- Score

365. Does application support password expiration?
<--- Score

366. Is per user profile settings something that should be put into the specification?
<--- Score

367. What functionality can be accessed without authentication?
<--- Score

368. How do you manage vulnerabilities?
<--- Score

369. What is web application penetration testing?
<--- Score

370. How will you communicate clear expectations regarding adherence to new policies and protocols?
<--- Score

371. Can organizations remediate vulnerabilities before exploitation?
<--- Score

372. How does your organizational policy influence how you manage updates if at all?
<--- Score

373. How do you ensure physical security?
<--- Score

374. What happens if a non administrative user tries to execute that request?
<--- Score

375. What type of addressing scheme is being used on the inside network?
<--- Score

376. Does migrate a monolithic system to microservices decreases the technical debt?
<--- Score

377. Which software security best practices are you familiar with?
<--- Score

378. Why is application verifier important?
<--- Score

379. How to catalogue and track approved components?
<--- Score

380. What will be the consequence of gaps in information when the initiative is rolled out?
<--- Score

381. Does the penetration tester have experience conducting application layer penetration testing?
<--- Score

382. Has it been the focus of media attention?
<--- Score

383. How will your code and applications react when something has gone wrong?
<--- Score

384. Are session management assets like user credentials and session IDs properly protected?
<--- Score

385. How to test for buffer overflow vulnerabilities?
<--- Score

386. What changes would you want to make to software updates?
<--- Score

387. How are business practices and human rights linked?
<--- Score

388. What are the responsibilities of your users for

handling updates?
<--- Score

389. Does your organization have a security operations function?
<--- Score

390. How do you handle security for machines?
<--- Score

391. How complex are security patches compared to other non security bug fixes?
<--- Score

392. What is the role of operational level grievance mechanisms?
<--- Score

393. Is your application security tool designed to keep up?
<--- Score

394. Do you know where all of your information assets reside?
<--- Score

395. What is an on site security assessment?
<--- Score

396. Is management prepared to react timely if a cybersecurity incident occurred?
<--- Score

397. What is the nature of the system/population being assessed?
<--- Score

398. Where are cti team members drawn from within your organization?
<--- Score

399. What is the name of your project?
<--- Score

400. Is your application missing the proper security hardening across any part of the application stack?
<--- Score

401. How does your threat model change by doing business with a partner organization?
<--- Score

402. How does the tool support the notion that certain roles may have different members for different assets?
<--- Score

403. Are stakeholders able to pull in security coaches for use on projects?
<--- Score

404. What is your value brought to the business?
<--- Score

405. Do security patches affect fewer functions than non security bug fixes?
<--- Score

406. Which tools are most effective in detecting security vulnerabilities?
<--- 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.

Vulnerability Remediation and Managing Projects, Criteria for Project Managers:

1.0 Initiating Process Group: Vulnerability Remediation

1. How can you make your needs known?

2. What are the short and long term implications?

3. What are the required resources?

4. Does the Vulnerability Remediation project team have enough people to execute the Vulnerability Remediation project plan?

5. Were resources available as planned?

6. Where must it be done?

7. Establishment of pm office?

8. Did the Vulnerability Remediation project team have the right skills?

9. If the risk event occurs, what will you do?

10. Do you know if the Vulnerability Remediation project requires outside equipment or vendor resources?

11. What were things that you did very well and want to do the same again on the next Vulnerability Remediation project?

12. How should needs be met?

13. For technology Vulnerability Remediation projects

only: Are all production support stakeholders (Business unit, technical support, & user) prepared for implementation with appropriate contingency plans?

14. Just how important is your work to the overall success of the Vulnerability Remediation project?

15. When must it be done?

16. What will you do?

17. At which cmmi level are software processes documented, standardized, and integrated into a standard to-be practiced process for your organization?

18. What are the inputs required to produce the deliverables?

19. Are you just doing busywork to pass the time?

1.1 Project Charter: Vulnerability Remediation

20. How high should you set your goals?

21. For whom?

22. Major high-level milestone targets: what events measure progress?

23. What date will the task finish?

24. Success determination factors: how will the success of the Vulnerability Remediation project be determined from the customers perspective?

25. When?

26. What are you trying to accomplish?

27. How much?

28. Vulnerability Remediation project objective statement: what must the Vulnerability Remediation project do?

29. Why Outsource?

30. What are the assumptions?

31. What is the most common tool for helping define the detail?

32. Environmental stewardship and sustainability considerations: what is the process that will be

used to ensure compliance with the environmental stewardship policy?

33. What is in it for you?

34. Assumptions and constraints: what assumptions were made in defining the Vulnerability Remediation project?

35. Pop quiz – which are the same inputs as in the Vulnerability Remediation project charter?

36. How are Vulnerability Remediation projects different from operations?

37. How will you know that a change is an improvement?

38. What material?

39. Why have you chosen the aim you have set forth?

1.2 Stakeholder Register: Vulnerability Remediation

40. How will reports be created?

41. What is the power of the stakeholder?

42. What & Why?

43. How big is the gap?

44. Who is managing stakeholder engagement?

45. What opportunities exist to provide communications?

46. How much influence do they have on the Vulnerability Remediation project?

47. How should employers make voices heard?

48. Who are the stakeholders?

49. Who wants to talk about Security?

50. What are the major Vulnerability Remediation project milestones requiring communications or providing communications opportunities?

51. Is your organization ready for change?

1.3 Stakeholder Analysis Matrix: Vulnerability Remediation

52. Business and product development?

53. How will the stakeholder directly benefit from the Vulnerability Remediation project and how will this affect the stakeholders motivation?

54. Who will be affected by the Vulnerability Remediation project?

55. How to measure the achievement of the Development Objective?

56. If you can not fix it, how do you do it differently?

57. Geographical, export, import?

58. Location and geographical?

59. Accreditations, etc?

60. Partnerships, agencies, distribution?

61. Who will be affected by the Vulnerability Remediation project?

62. Are they likely to influence the success or failure of your Vulnerability Remediation project?

63. Morale, commitment, leadership?

64. Who has control over whom?

65. What are the opportunities for communication?

66. What is the stakeholders power and status in relation to the Vulnerability Remediation project?

67. Lack of competitive strength?

68. Processes and systems, etc?

69. Contributions to policy and practice?

70. Will the impacts be local, national or international?

71. Why is it important to identify them?

2.0 Planning Process Group: Vulnerability Remediation

72. Explanation: is what the Vulnerability Remediation project intents to solve a hard question?

73. How are the principles of aid effectiveness (ownership, alignment, management for development results and mutual responsibility) being applied in the Vulnerability Remediation project?

74. What do you need to do?

75. How well defined and documented are the Vulnerability Remediation project management processes you chose to use?

76. In what ways can the governance of the Vulnerability Remediation project be improved so that it has greater likelihood of achieving future sustainability?

77. How does activity resource estimation affect activity duration estimation?

78. To what extent do the intervention objectives and strategies of the Vulnerability Remediation project respond to your organizations plans?

79. Is the schedule for the set products being met?

80. What good practices or successful experiences or transferable examples have been identified?

81. What is the critical path for this Vulnerability

Remediation project, and what is the duration of the critical path?

82. To what extent are the visions and actions of the partners consistent or divergent with regard to the program?

83. To what extent have public/private national resources and/or counterparts been mobilized to contribute to the programs objective and produce results and impacts?

84. On which process should team members spend the most time?

85. Does it make any difference if you are successful?

86. When will the Vulnerability Remediation project be done?

87. If a task is partitionable, is this a sufficient condition to reduce the Vulnerability Remediation project duration?

88. How well do the team follow the chosen processes?

89. What should you do next?

90. You are creating your WBS and find that you keep decomposing tasks into smaller and smaller units. How can you tell when you are done?

2.1 Project Management Plan: Vulnerability Remediation

91. What would you do differently?

92. Who manages integration?

93. How can you best help your organization to develop consistent practices in Vulnerability Remediation project management planning stages?

94. Is there an incremental analysis/cost effectiveness analysis of proposed mitigation features based on an approved method and using an accepted model?

95. What should you drop in order to add something new?

96. Are comparable cost estimates used for comparing, screening and selecting alternative plans, and has a reasonable cost estimate been developed for the recommended plan?

97. Do the proposed changes from the Vulnerability Remediation project include any significant risks to safety?

98. Are cost risk analysis methods applied to develop contingencies for the estimated total Vulnerability Remediation project costs?

99. What worked well?

100. What went right?

101. Are there any client staffing expectations?

102. What went wrong?

103. What is the justification?

104. Are the existing and future without-plan conditions reasonable and appropriate?

105. What data/reports/tools/etc. do your PMs need?

106. Are alternatives safe, functional, constructible, economical, reasonable and sustainable?

107. What if, for example, the positive direction and vision of your organization causes expected trends to change resulting in greater need than expected?

108. Who is the sponsor?

109. What is risk management?

2.2 Scope Management Plan: Vulnerability Remediation

110. How do you know how you are doing?

111. Is there a scope management plan that includes how Vulnerability Remediation project scope will be defined, developed, monitored, validated and controlled?

112. Is the quality assurance team identified?

113. Does the implementation plan have an appropriate division of responsibilities?

114. Were Vulnerability Remediation project team members involved in detailed estimating and scheduling?

115. Are software metrics formally captured, analyzed and used as a basis for other Vulnerability Remediation project estimates?

116. Why is a scope management plan important?

117. Pop quiz – which are the same inputs as in scope planning?

118. Is the communication plan being followed?

119. Was the scope definition used in task sequencing?

120. Are any non-compliance issues that exist due to organizations practices?

121. Is there a formal process for updating the Vulnerability Remediation project baseline?

122. Is the Vulnerability Remediation project status reviewed with the steering and executive teams at appropriate intervals?

123. Pop quiz – what changed on Vulnerability Remediation project scope statement input?

124. What is the need the Vulnerability Remediation project will address?

125. Is there an on-going process in place to monitor Vulnerability Remediation project risks?

126. Product – what are you trying to accomplish and how will you know when you are finished?

127. Have the key functions and capabilities been defined and assigned to each release or iteration?

128. Are updated Vulnerability Remediation project time & resource estimates reasonable based on the current Vulnerability Remediation project stage?

2.3 Requirements Management Plan: Vulnerability Remediation

129. Did you distinguish the scope of work the contractor(s) will be required to do?

130. Did you use declarative statements?

131. Do you expect stakeholders to be cooperative?

132. Who is responsible for quantifying the Vulnerability Remediation project requirements?

133. What performance metrics will be used?

134. Do you really need to write this document at all?

135. Has the requirements team been instructed in the Change Control process?

136. Who has the authority to reject Vulnerability Remediation project requirements?

137. Controlling Vulnerability Remediation project requirements involves monitoring the status of the Vulnerability Remediation project requirements and managing changes to the requirements. Who is responsible for monitoring and tracking the Vulnerability Remediation project requirements?

138. Who came up with this requirement?

139. Are all the stakeholders ready for the transition into the user community?

140. Do you have an appropriate arrangement for meetings?

141. Is there formal agreement on who has authority to request a change in requirements?

142. After the requirements are gathered and set forth on the requirements register, theyre little more than a laundry list of items. Some may be duplicates, some might conflict with others and some will be too broad or too vague to understand. Describe how the requirements will be analyzed. Who will perform the analysis?

143. Do you have an agreed upon process for alerting the Vulnerability Remediation project Manager if a request for change in requirements leads to a product scope change?

144. Is infrastructure setup part of your Vulnerability Remediation project?

145. Business analysis scope?

146. What cost metrics will be used?

147. When and how will a requirements baseline be established in this Vulnerability Remediation project?

2.4 Requirements Documentation: Vulnerability Remediation

148. Completeness. are all functions required by the customer included?

149. Has requirements gathering uncovered information that would necessitate changes?

150. What are current process problems?

151. Can the requirement be changed without a large impact on other requirements?

152. Have the benefits identified with the system being identified clearly?

153. What is the risk associated with the technology?

154. What can tools do for us?

155. Do your constraints stand?

156. How to document system requirements?

157. Is the requirement properly understood?

158. What variations exist for a process?

159. What are the attributes of a customer?

160. Is your business case still valid?

161. If applicable; are there issues linked with the fact that this is an offshore Vulnerability Remediation

project?

162. What marketing channels do you want to use: e-mail, letter or sms?

163. Are there legal issues?

164. What will be the integration problems?

165. Verifiability. can the requirements be checked?

166. Is the origin of the requirement clearly stated?

167. What are the potential disadvantages/ advantages?

2.5 Requirements Traceability Matrix: Vulnerability Remediation

168. Is there a requirements traceability process in place?

169. What percentage of Vulnerability Remediation projects are producing traceability matrices between requirements and other work products?

170. Describe the process for approving requirements so they can be added to the traceability matrix and Vulnerability Remediation project work can be performed. Will the Vulnerability Remediation project requirements become approved in writing?

171. Do you have a clear understanding of all subcontracts in place?

172. What are the chronologies, contingencies, consequences, criteria?

173. Why use a WBS?

174. Will you use a Requirements Traceability Matrix?

175. How will it affect the stakeholders personally in career?

176. What is the WBS?

177. How small is small enough?

178. How do you manage scope?

179. Why do you manage scope?

2.6 Project Scope Statement: Vulnerability Remediation

180. Who will you recommend approve the change, and when do you recommend the change reviews occur?

181. Will all Vulnerability Remediation project issues be unconditionally tracked through the issue resolution process?

182. Have the configuration management functions been assigned?

183. Will statistics related to QA be collected, trends analyzed, and problems raised as issues?

184. What are the defined meeting materials?

185. Is the plan under configuration management?

186. Was planning completed before the Vulnerability Remediation project was initiated?

187. Have you been able to thoroughly document the Vulnerability Remediation projects assumptions and constraints?

188. Will the risk status be reported to management on a regular and frequent basis?

189. Elements that deal with providing the detail?

190. Why do you need to manage scope?

191. Will the risk plan be updated on a regular and frequent basis?

192. Will tasks be marked complete only after QA has been successfully completed?

193. Is an issue management process documented and filed?

194. What is a process you might recommend to verify the accuracy of the research deliverable?

195. Elements of scope management that deal with concept development ?

2.7 Assumption and Constraint Log: Vulnerability Remediation

196. Is there adequate stakeholder participation for the vetting of requirements definition, changes and management?

197. Does a specific action and/or state that is known to violate security policy occur?

198. How are new requirements or changes to requirements identified?

199. Contradictory information between document sections?

200. What would you gain if you spent time working to improve this process?

201. Are there processes defining how software will be developed including development methods, overall timeline for development, software product standards, and traceability?

202. No superfluous information or marketing narrative?

203. How can you prevent/fix violations?

204. Are processes for release management of new development from coding and unit testing, to integration testing, to training, and production defined and followed?

205. How do you design an auditing system?

206. Are there standards for code development?

207. After observing execution of process, is it in compliance with the documented Plan?

208. Is staff trained on the software technologies that are being used on the Vulnerability Remediation project?

209. What weaknesses do you have?

210. Was the document/deliverable developed per the appropriate or required standards (for example, Institute of Electrical and Electronics Engineers standards)?

211. What does an audit system look like?

212. What do you audit?

213. Contradictory information between different documents?

214. Does the system design reflect the requirements?

2.8 Work Breakdown Structure: Vulnerability Remediation

215. Is it still viable?

216. Who has to do it?

217. How much detail?

218. What is the probability of completing the Vulnerability Remediation project in less that xx days?

219. Can you make it?

220. Where does it take place?

221. Do you need another level?

222. Is the work breakdown structure (wbs) defined and is the scope of the Vulnerability Remediation project clear with assigned deliverable owners?

223. What has to be done?

224. Why would you develop a Work Breakdown Structure?

225. When would you develop a Work Breakdown Structure?

226. How many levels?

227. How big is a work-package?

228. Is it a change in scope?

229. Why is it useful?

230. When does it have to be done?

231. How far down?

2.9 WBS Dictionary: Vulnerability Remediation

232. Are the wbs and organizational levels for application of the Vulnerability Remediation projected overhead costs identified?

233. Do procedures specify under what circumstances replanning of open work packages may occur, and the methods to be followed?

234. Are the responsibilities and authorities of each of the above organizational elements or managers clearly defined?

235. Are authorized changes being incorporated in a timely manner?

236. The already stated responsible for overhead performance control of related costs?

237. Are records maintained to show full accountability for all material purchased for the contract, including the residual inventory?

238. Contemplated overhead expenditure for each period based on the best information currently available?

239. The total budget for the contract (including estimates for authorized and unpriced work)?

240. Is cost performance measurement at the point in time most suitable for the category of material involved, and no earlier than the time of actual receipt

of material?

241. Is work progressively subdivided into detailed work packages as requirements are defined?

242. Are the procedures for identifying indirect costs to incurring organizations, indirect cost pools, and allocating the costs from the pools to the contracts formally documented?

243. Does the cost accumulation system provide for summarization of indirect costs from the point of allocation to the contract total?

244. Changes in the current direct and Vulnerability Remediation projected base?

245. Can the contractor substantiate work package and planning package budgets?

246. Are work packages reasonably short in time duration or do they have adequate objective indicators/milestones to minimize subjectivity of the in process work evaluation?

247. What is the end result of a work package?

248. Is authorization of budgets in excess of the contract budget base controlled formally and done with the full knowledge and recognition of the procuring activity?

249. Are internal budgets for authorized, and not priced changes based on the contractors resource plan for accomplishing the work?

250. Detailed schedules which support control account and work package start and completion dates/events?

251. Is the work done on a work package level as described in the WBS dictionary?

2.10 Schedule Management Plan: Vulnerability Remediation

252. Are internal Vulnerability Remediation project status meetings held at reasonable intervals?

253. Has the business need been clearly defined?

254. Are the predecessor and successor relationships accurate?

255. Are enough systems & user personnel assigned to the Vulnerability Remediation project?

256. Does the schedule have reasonable float?

257. Has the scope management document been updated and distributed to help prevent scope creep?

258. Is the ims development and management approach described?

259. Does all Vulnerability Remediation project documentation reside in a common repository for easy access?

260. Are metrics used to evaluate and manage Vendors?

261. Is there a set of procedures defining the scope, procedures, and deliverables defining quality control?

262. Are all activities captured and do they address all approved work scope in the Vulnerability Remediation project baseline?

263. Is the development plan and/or process documented?

264. Have Vulnerability Remediation project success criteria been defined?

265. What will be the final cost of the Vulnerability Remediation project if status quo is maintained?

266. Are all resource assumptions documented?

267. Sensitivity analysis?

268. Have key stakeholders been identified?

269. Has your organization readiness assessment been conducted?

270. Are all attributes of the activities defined, including risk and uncertainty?

271. Pareto diagrams, statistical sampling, flow charting or trend analysis used quality monitoring?

2.11 Activity List: Vulnerability Remediation

272. When will the work be performed?

273. How should ongoing costs be monitored to try to keep the Vulnerability Remediation project within budget?

274. In what sequence?

275. How much slack is available in the Vulnerability Remediation project?

276. How difficult will it be to do specific activities on this Vulnerability Remediation project?

277. What is your organizations history in doing similar activities?

278. What is the total time required to complete the Vulnerability Remediation project if no delays occur?

279. Where will it be performed?

280. Is there anything planned that does not need to be here?

281. What are the critical bottleneck activities?

282. What did not go as well?

283. How do you determine the late start (LS) for each activity?

284. How will it be performed?

285. What went well?

286. Are the required resources available or need to be acquired?

287. What is the LF and LS for each activity?

288. For other activities, how much delay can be tolerated?

289. Should you include sub-activities?

290. The wbs is developed as part of a joint planning session. and how do you know that youhave done this right?

2.12 Activity Attributes: Vulnerability Remediation

291. Were there other ways you could have organized the data to achieve similar results?

292. Do you feel very comfortable with your prediction?

293. Can more resources be added?

294. Is there a trend during the year?

295. Does your organization of the data change its meaning?

296. What is the general pattern here?

297. Activity: what is Missing?

298. Resource is assigned to?

299. How else could the items be grouped?

300. Have you identified the Activity Leveling Priority code value on each activity?

301. Resources to accomplish the work?

302. Has management defined a definite timeframe for the turnaround or Vulnerability Remediation project window?

303. Would you consider either of corresponding activities an outlier?

304. What is missing?

305. Which method produces the more accurate cost assignment?

306. Time for overtime?

307. Can you re-assign any activities to another resource to resolve an over-allocation?

2.13 Milestone List: Vulnerability Remediation

308. Legislative effects?

309. It is to be a narrative text providing the crucial aspects of your Vulnerability Remediation project proposal answering what, who, how, when and where?

310. Political effects?

311. Continuity, supply chain robustness?

312. How late can the activity finish?

313. Environmental effects?

314. What specific improvements did you make to the Vulnerability Remediation project proposal since the previous time?

315. Describe the industry you are in and the market growth opportunities. What is the market for your technology, product or service?

316. Loss of key staff?

317. How soon can the activity start?

318. How will the milestone be verified?

319. What has been done so far?

320. How do you manage time?

321. Marketing - reach, distribution, awareness?

322. What would happen if a delivery of material was one week late?

323. How difficult will it be to do specific activities on this Vulnerability Remediation project?

324. Reliability of data, plan predictability?

325. Calculate how long can activity be delayed?

2.14 Network Diagram: Vulnerability Remediation

326. Are the gantt chart and/or network diagram updated periodically and used to assess the overall Vulnerability Remediation project timetable?

327. Why must you schedule milestones, such as reviews, throughout the Vulnerability Remediation project?

328. What is the probability of completing the Vulnerability Remediation project in less that xx days?

329. How confident can you be in your milestone dates and the delivery date?

330. Review the logical flow of the network diagram. Take a look at which activities you have first and then sequence the activities. Do they make sense?

331. What is the lowest cost to complete this Vulnerability Remediation project in xx weeks?

332. What job or jobs precede it?

333. What are the Key Success Factors?

334. What to do and When?

335. Can you calculate the confidence level?

336. If the Vulnerability Remediation project network diagram cannot change and you have extra personnel resources, what is the BEST thing to do?

337. What job or jobs follow it?

338. What can be done concurrently?

339. What are the Major Administrative Issues?

340. What job or jobs could run concurrently?

341. What controls the start and finish of a job?

342. What activities must follow this activity?

343. Where do schedules come from?

344. What activities must occur simultaneously with this activity?

2.15 Activity Resource Requirements: Vulnerability Remediation

345. How do you handle petty cash?

346. Other support in specific areas?

347. What are constraints that you might find during the Human Resource Planning process?

348. Why do you do that?

349. Which logical relationship does the PDM use most often?

350. Do you use tools like decomposition and rolling-wave planning to produce the activity list and other outputs?

351. When does monitoring begin?

352. Anything else?

353. Are there unresolved issues that need to be addressed?

354. Organizational Applicability?

355. What is the Work Plan Standard?

356. How many signatures do you require on a check and does this match what is in your policy and procedures?

2.16 Resource Breakdown Structure: Vulnerability Remediation

357. Who will use the system?

358. The list could probably go on, but, the thing that you would most like to know is, How long & How much?

359. What is the number one predictor of a groups productivity?

360. Who needs what information?

361. Who delivers the information?

362. How difficult will it be to do specific activities on this Vulnerability Remediation project?

363. Who is allowed to perform which functions?

364. Which resource planning tool provides information on resource responsibility and accountability?

365. What is the primary purpose of the human resource plan?

366. What defines a successful Vulnerability Remediation project?

367. When do they need the information?

368. How should the information be delivered?

369. Why do you do it?

370. Are the required resources available?

371. What defines a successful Vulnerability Remediation project?

372. What can you do to improve productivity?

373. Goals for the Vulnerability Remediation project. What is each stakeholders desired outcome for the Vulnerability Remediation project?

2.17 Activity Duration Estimates: Vulnerability Remediation

374. Why is activity definition the first process involved in Vulnerability Remediation project time management?

375. Does a process exist to determine the potential loss or gain if risk events occur?

376. If you plan to take the PMP exam soon, what should you do to prepare?

377. Account for the four frames of organizations. How can they help Vulnerability Remediation project managers understand your organizational context for Vulnerability Remediation projects?

378. What are the main types of contracts if you do decide to outsource?

379. How could you use each technique in your organization?

380. Are contingency plans created to prepare for risk events to occur?

381. What are the main types of goods and services being outsourced?

382. Are resource rates available to calculate Vulnerability Remediation project costs?

383. What is the career outlook for Vulnerability Remediation project managers in information

technology?

384. What are the largest companies that provide information technology outsourcing services?

385. Consider the changes in the job market for information technology workers. How does the job market and current state of the economy affect human resource management?

386. What type of people would you want on your team?

387. How can you use Microsoft Vulnerability Remediation project and Excel to assist in Vulnerability Remediation project risk management?

388. Are actual Vulnerability Remediation project results compared with planned or expected results to determine the variance?

389. Is risk identification completed regularly throughout the Vulnerability Remediation project?

390. How could you define throughput and how would your organization benefit from maximizing it?

391. What does it mean to take a systems view of a Vulnerability Remediation project?

392. Why is it important to determine activity sequencing on Vulnerability Remediation projects?

393. What tasks must follow this task?

2.18 Duration Estimating Worksheet: Vulnerability Remediation

394. Science = process: remember the scientific method?

395. Is a construction detail attached (to aid in explanation)?

396. What work will be included in the Vulnerability Remediation project?

397. Why estimate time and cost?

398. When does your organization expect to be able to complete it?

399. Why estimate costs?

400. Is this operation cost effective?

401. What is your role?

402. What is the total time required to complete the Vulnerability Remediation project if no delays occur?

403. What is an Average Vulnerability Remediation project?

404. How can the Vulnerability Remediation project be displayed graphically to better visualize the activities?

405. Will the Vulnerability Remediation project collaborate with the local community and leverage

resources?

406. Value pocket identification & quantification what are value pockets?

407. How should ongoing costs be monitored to try to keep the Vulnerability Remediation project within budget?

408. What utility impacts are there?

409. Is the Vulnerability Remediation project responsive to community need?

410. Do any colleagues have experience with your organization and/or RFPs?

2.19 Project Schedule: Vulnerability Remediation

411. Month Vulnerability Remediation project take?

412. Are activities connected because logic dictates the order in which others occur?

413. How can slack be negative?

414. Did the Vulnerability Remediation project come in on schedule?

415. How do you manage Vulnerability Remediation project Risk?

416. How does a Vulnerability Remediation project get to be a year late ?

417. Verify that the update is accurate. Are all remaining durations correct?

418. What is the purpose of a Vulnerability Remediation project schedule?

419. How do you know that youhave done this right?

420. Are key risk mitigation strategies added to the Vulnerability Remediation project schedule?

421. Are all remaining durations correct?

422. Are you working on the right risks?

423. Activity charts and bar charts are graphical

representations of a Vulnerability Remediation project schedule ...how do they differ?

424. Is the Vulnerability Remediation project schedule available for all Vulnerability Remediation project team members to review?

425. Are there activities that came from a template or previous Vulnerability Remediation project that are not applicable on this phase of this Vulnerability Remediation project?

426. Did the Vulnerability Remediation project come in under budget?

427. Does the condition or event threaten the Vulnerability Remediation projects objectives in any ways?

2.20 Cost Management Plan: Vulnerability Remediation

428. Does all Vulnerability Remediation project documentation reside in a common repository for easy access?

429. Are changes in scope (deliverable commitments) agreed to by all affected groups & individuals?

430. Are decisions captured in a decisions log?

431. Is your organization certified as a supplier, wholesaler, regular dealer, or manufacturer of corresponding products/supplies?

432. Vulnerability Remediation project definition & scope?

433. Are vendor contract reports, reviews and visits conducted periodically?

434. Are updated Vulnerability Remediation project time & resource estimates reasonable based on the current Vulnerability Remediation project stage?

435. Is it possible to track all classes of Vulnerability Remediation project work (e.g. scheduled, un-scheduled, defect repair, etc.)?

436. Have all documents been archived in a Vulnerability Remediation project repository for each release?

437. Was your organizations estimating methodology

being used and followed?

438. Scope of work – What is the scope of work for each of the planned contracts?

439. Have stakeholder accountabilities & responsibilities been clearly defined?

440. Contingency – how will cost contingency be administered?

441. Staffing Requirements?

442. Technical and functional?

443. Are risk oriented checklists used during risk identification?

444. Has a capability assessment been conducted?

445. Are actuals compared against estimates to analyze and correct variances?

446. Are quality inspections and review activities listed in the Vulnerability Remediation project schedule(s)?

2.21 Activity Cost Estimates: Vulnerability Remediation

447. Maintenance Reserve?

448. Were decisions made in a timely manner?

449. Performance bond should always provide what part of the contract value?

450. What is included in indirect cost being allocated?

451. Certification of actual expenditures?

452. Does the estimator estimate by task or by person?

453. What procedures are put in place regarding bidding and cost comparisons, if any?

454. What cost data should be used to estimate costs during the 2-year follow-up period?

455. Review – what are some common errors in activities to avoid?

456. Is there anything unique in this Vulnerability Remediation projects scope statement that will affect resources?

457. How do you do activity recasts?

458. What defines a successful Vulnerability Remediation project?

459. How do you manage cost?

460. What do you want to know about the stay to know if costs were inappropriately high or low?

461. Can you change your activities?

462. Are cost subtotals needed?

463. Would you hire them again?

464. Is costing method consistent with study goals?

465. Will you need to provide essential services information about activities?

2.22 Cost Estimating Worksheet: Vulnerability Remediation

466. What can be included?

467. What additional Vulnerability Remediation project(s) could be initiated as a result of this Vulnerability Remediation project?

468. What will others want?

469. Is the Vulnerability Remediation project responsive to community need?

470. Ask: are others positioned to know, are others credible, and will others cooperate?

471. What is the purpose of estimating?

472. What costs are to be estimated?

473. Does the Vulnerability Remediation project provide innovative ways for stakeholders to overcome obstacles or deliver better outcomes?

474. What info is needed?

475. Identify the timeframe necessary to monitor progress and collect data to determine how the selected measure has changed?

476. What is the estimated labor cost today based upon this information?

477. Will the Vulnerability Remediation project

collaborate with the local community and leverage resources?

478. Is it feasible to establish a control group arrangement?

479. Who is best positioned to know and assist in identifying corresponding factors?

480. Can a trend be established from historical performance data on the selected measure and are the criteria for using trend analysis or forecasting methods met?

481. What happens to any remaining funds not used?

482. How will the results be shared and to whom?

2.23 Cost Baseline: Vulnerability Remediation

483. Verify business objectives. Are others appropriate, and well-articulated?

484. Review your risk triggers -have your risks changed?

485. Has operations management formally accepted responsibility for operating and maintaining the product(s) or service(s) delivered by the Vulnerability Remediation project?

486. What is it ?

487. How likely is it to go wrong?

488. Escalation criteria met?

489. How difficult will it be to do specific tasks on the Vulnerability Remediation project?

490. Have all the product or service deliverables been accepted by the customer?

491. Are you asking management for something as a result of this update?

492. Has the appropriate access to relevant data and analysis capability been granted?

493. Are you meeting with your team regularly?

494. Have the resources used by the Vulnerability

Remediation project been reassigned to other units or Vulnerability Remediation projects?

495. When should cost estimates be developed?

496. Has the Vulnerability Remediation project documentation been archived or otherwise disposed as described in the Vulnerability Remediation project communication plan?

497. Will the Vulnerability Remediation project fail if the change request is not executed?

498. Is there anything unique in this Vulnerability Remediation projects scope statement that will affect resources?

499. Has the Vulnerability Remediation project (or Vulnerability Remediation project phase) been evaluated against each objective established in the product description and Integrated Vulnerability Remediation project Plan?

500. How long are you willing to wait before you find out were late?

501. What would the life cycle costs be?

502. Have all approved changes to the Vulnerability Remediation project requirement been identified and impact on the performance, cost, and schedule baselines documented?

2.24 Quality Management Plan: Vulnerability Remediation

503. Are there trends or hot spots?

504. Who is responsible for writing the qapp?

505. How are senior leaders, employees, and your organization involved in supporting the community?

506. Was trending evident between audits?

507. What methods are used?

508. What data do you gather/use/compile?

509. Are requirements management tracking tools and procedures in place?

510. How do you decide what information needs to be recorded?

511. What are your organizations current levels and trends for the already stated measures related to customer satisfaction/ dissatisfaction and product/ service performance?

512. What are the appropriate test methods to be used?

513. What does it do for you (or to me)?

514. Are you following the quality standards?

515. What is quality and how will you ensure it?

516. List your organizations customer contact standards that employees are expected to maintain. How are corresponding standards measured?

517. When reporting to different audiences, do you vary the form or type of report?

518. How do senior leaders create and communicate values and performance expectations?

519. Have you eliminated all duplicative tasks or manual efforts, where appropriate?

520. How is staff trained on the recording of field notes?

521. What is the return on investment?

522. Results Available?

2.25 Quality Metrics: Vulnerability Remediation

523. What about still open problems?

524. How do you measure?

525. What metrics are important and most beneficial to measure?

526. Where is quality now?

527. Filter visualizations of interest?

528. What does this tell us?

529. What do you measure?

530. If the defect rate during testing is substantially higher than that of the previous release (or a similar product), then ask: Did you plan for and actually improve testing effectiveness?

531. Was material distributed on time?

532. Which are the right metrics to use?

533. How are requirements conflicts resolved?

534. Is there a set of procedures to capture, analyze and act on quality metrics?

535. What if the biggest risk to your business were the already stated people who do not complain?

536. Are quality metrics defined?

537. What method of measurement do you use?

538. How do you know if everyone is trying to improve the right things?

539. Is quality culture a competitive advantage?

2.26 Process Improvement Plan: Vulnerability Remediation

540. Have the supporting tools been developed or acquired?

541. Where do you want to be?

542. Where are you now?

543. Have the frequency of collection and the points in the process where measurements will be made been determined?

544. Does your process ensure quality?

545. Are you making progress on your improvement plan?

546. What is the test-cycle concept?

547. How do you manage quality?

548. Are you making progress on the goals?

549. What lessons have you learned so far?

550. The motive is determined by asking, Why do you want to achieve this goal?

551. Management commitment at all levels?

552. Purpose of goal: the motive is determined by asking, why do you want to achieve this goal?

553. Are you making progress on the improvement framework?

554. Where do you focus?

555. Everyone agrees on what process improvement is, right?

2.27 Responsibility Assignment Matrix: Vulnerability Remediation

556. Is it safe to say you can handle more work or that some tasks you are supposed to do arent worth doing?

557. What are the constraints?

558. The staff characteristics – is the group or the person capable to work together as a team?

559. Past experience – the person or the group worked at something similar in the past?

560. All cwbs elements specified for external reporting?

561. What does wbs accomplish?

562. Are others working on the right things?

563. Are people afraid to let you know when others are under allocated?

564. Are too many reports done in writing instead of verbally?

565. What cost control tool do many experts say is crucial to Vulnerability Remediation project management?

566. Ideas for developing soft skills at your organization?

567. Not any rs, as, or cs: if an identified role is only informed, should others be eliminated from the matrix?

568. Too many rs: with too many people labeled as doing the work, are there too many hands involved?

569. Who is going to do that work?

570. Is the entire contract planned in time-phased control accounts to the extent practicable?

571. Are all elements of indirect expense identified to overhead cost budgets of Vulnerability Remediation projections?

572. The anticipated business volume?

573. Are records maintained to show how undistributed budgets are controlled?

574. Direct labor dollars and/or hours?

2.28 Roles and Responsibilities: Vulnerability Remediation

575. Have you ever been a part of this team?

576. What are your major roles and responsibilities in the area of performance measurement and assessment?

577. What should you highlight for improvement?

578. What areas of supervision are challenging for you?

579. Be specific; avoid generalities. Thank you and great work alone are insufficient. What exactly do you appreciate and why?

580. Are Vulnerability Remediation project team roles and responsibilities identified and documented?

581. Are your policies supportive of a culture of quality data?

582. Implementation of actions: Who are the responsible units?

583. What expectations were met?

584. Does your vision/mission support a culture of quality data?

585. What areas would you highlight for changes or improvements?

586. Once the responsibilities are defined for the Vulnerability Remediation project, have the deliverables, roles and responsibilities been clearly communicated to every participant?

587. Influence: what areas of organizational decision making are you able to influence when you do not have authority to make the final decision?

588. Who: who is involved?

589. Is there a training program in place for stakeholders covering expectations, roles and responsibilities and any addition knowledge others need to be good stakeholders?

590. Was the expectation clearly communicated?

591. What should you do now to ensure that you are meeting all expectations of your current position?

592. Where are you most strong as a supervisor?

593. Accountabilities: what are the roles and responsibilities of individual team members?

594. What should you do now to prepare yourself for a promotion, increased responsibilities or a different job?

2.29 Human Resource Management Plan: Vulnerability Remediation

595. How are you going to ensure that you have a well motivated workforce?

596. How does the proposed individual meet each requirement?

597. What areas were overlooked on this Vulnerability Remediation project?

598. Are issues raised, assessed, actioned, and resolved in a timely and efficient manner?

599. Are parking lot items captured?

600. Has the Vulnerability Remediation project manager been identified?

601. Are changes in deliverable commitments agreed to by all affected groups & individuals?

602. Is there a Steering Committee in place?

603. Has a provision been made to reassess Vulnerability Remediation project risks at various Vulnerability Remediation project stages?

604. Is an industry recognized support tool(s) being used for Vulnerability Remediation project scheduling & tracking?

605. Are meeting minutes captured and sent out after the meeting?

606. Are there checklists created to determine if all quality processes are followed?

607. Is quality monitored from the perspective of the customers needs and expectations?

608. Is there an approved case?

609. Are non-critical path items updated and agreed upon with the teams?

610. Is a pmo (Vulnerability Remediation project management office) in place and provide oversight to the Vulnerability Remediation project?

611. Alignment to strategic goals & objectives?

612. Were stakeholders aware and supportive of the principles and practices of modern cost estimation?

613. Does a documented Vulnerability Remediation project organizational policy & plan (i.e. governance model) exist?

2.30 Communications Management Plan: Vulnerability Remediation

614. Will messages be directly related to the release strategy or phases of the Vulnerability Remediation project?

615. What is Vulnerability Remediation project communications management?

616. Do you then often overlook a key stakeholder or stakeholder group?

617. Where do team members get information?

618. What is the stakeholders level of authority?

619. What does the stakeholder need from the team?

620. What to learn?

621. Are others needed?

622. Are stakeholders internal or external?

623. Timing: when do the effects of the communication take place?

624. What help do you and your team need from the stakeholder?

625. How were corresponding initiatives successful?

626. Do you feel a register helps?

627. Do you feel more overwhelmed by stakeholders?

628. What to know?

629. Are there too many who have an interest in some aspect of your work?

630. Is the stakeholder role recognized by your organization?

631. Are there potential barriers between the team and the stakeholder?

632. Why do you manage communications?

633. Why is stakeholder engagement important?

2.31 Risk Management Plan: Vulnerability Remediation

634. How do you manage Vulnerability Remediation project Risk?

635. Anticipated volatility of the requirements?

636. Have customers been involved fully in the definition of requirements?

637. Market risk: will the new product be useful to your organization or marketable to others?

638. People risk -are people with appropriate skills available to help complete the Vulnerability Remediation project?

639. How risk averse are you?

640. Premium on reliability of product?

641. Are team members trained in the use of the tools?

642. How much risk protection can you afford?

643. Do you train all developers in the process?

644. Number of users of the product?

645. Risk documentation: what reporting formats and processes will be used for risk management activities?

646. Is the customer willing to participate in reviews?

647. What is the likelihood that your organization would accept responsibility for the risk?

648. What is the likelihood?

649. How much risk can you tolerate?

650. Where do risks appear in the business phases?

651. Is a software Vulnerability Remediation project management tool available?

2.32 Risk Register: Vulnerability Remediation

652. Does the evidence highlight any areas to advance opportunities or foster good relations. If yes what steps will be taken?

653. Methodology: how will risk management be performed on this Vulnerability Remediation project?

654. What is the appropriate level of risk management for this Vulnerability Remediation project?

655. Are there any gaps in the evidence?

656. Cost/benefit – how much will the proposed mitigations cost and how does this cost compare with the potential cost of the risk event/situation should it occur?

657. Are corrective measures implemented as planned?

658. Have other controls and solutions been implemented in other services which could be applied as an alternative to additional funding?

659. What is the reason for current performance gaps and do the risks and opportunities identified previously account for this?

660. Schedule impact/severity estimated range (workdays) assume the event happens, what is the potential impact?

661. Having taken action, how did the responses effect change, and where is the Vulnerability Remediation project now?

662. What should you do now?

663. Who needs to know about this?

664. What is your current and future risk profile?

665. What is a Risk?

666. User involvement: do you have the right users?

667. How could corresponding Risk affect the Vulnerability Remediation project in terms of cost and schedule?

668. When is it going to be done?

669. How are risks identified?

670. Who is going to do it?

2.33 Probability and Impact Assessment: Vulnerability Remediation

671. Are staff committed for the duration of the Vulnerability Remediation project?

672. What will be the likely political environment during the life of the Vulnerability Remediation project?

673. My Vulnerability Remediation project leader has suddenly left your organization, what do you do?

674. What new technologies are being explored in the same area?

675. Can the Vulnerability Remediation project proceed without assuming the risk?

676. Can you avoid altogether some things that might go wrong?

677. Which risks need to move on to Perform Quantitative Risk Analysis?

678. What are the current requirements of the customer?

679. What is the likely future demand of the customer?

680. Do you have specific methods that you use for each phase of the process?

681. What can you do to minimize the impact if it does?

682. What are the likely future requirements?

683. Is the delay in one subVulnerability Remediation project going to affect another?

684. Management -what contingency plans do you have if the risk becomes a reality?

685. Which of your Vulnerability Remediation projects should be selected when compared with other Vulnerability Remediation projects?

686. What is the likelihood of a breakthrough?

687. Who should be notified of the occurrence of each of the risk indicators?

688. Do the requirements require the creation of new algorithms?

689. What will be the environmental impact of the Vulnerability Remediation project?

2.34 Probability and Impact Matrix: Vulnerability Remediation

690. What will be the impact or consequence if the risk occurs?

691. Have you worked with the customer in the past?

692. Are tools for analysis and design available?

693. What has the Vulnerability Remediation project manager forgotten to do?

694. Can it be changed quickly?

695. The customer requests a change to the Vulnerability Remediation project that would increase the Vulnerability Remediation project risk. Which should you do before ass the others?

696. How is the Vulnerability Remediation project going to be managed?

697. What should be done with risks on the watch list?

698. Who is going to be the consortium leader?

699. Are enough people available?

700. What will be the likely political environment during the life of the Vulnerability Remediation project?

701. How well is the risk understood?

702. What will be the likely incidence of conflict with neighboring Vulnerability Remediation projects?

703. Are flexibility and reuse paramount?

704. Are compilers and code generators available and suitable for the product to be built?

705. Risk may be made during which step of risk management?

706. Have top software and customer managers formally committed to support the Vulnerability Remediation project?

707. Can you handle the investment risk?

2.35 Risk Data Sheet: Vulnerability Remediation

708. What are you weak at and therefore need to do better?

709. How can it happen?

710. Type of risk identified?

711. Has the most cost-effective solution been chosen?

712. What will be the consequences if it happens?

713. What if client refuses?

714. What are you trying to achieve (Objectives)?

715. Are new hazards created?

716. If it happens, what are the consequences?

717. What can you do?

718. What can happen?

719. What are the main opportunities available to you that you should grab while you can?

720. Whom do you serve (customers)?

721. Potential for recurrence?

722. Has a sensitivity analysis been carried out?

723. How do you handle product safely?

724. What are the main threats to your existence?

2.36 Procurement Management Plan: Vulnerability Remediation

725. Have all documents been archived in a Vulnerability Remediation project repository for each release?

726. What areas does the group agree are the biggest success on the Vulnerability Remediation project?

727. Has a structured approach been used to break work effort into manageable components (WBS)?

728. Are quality inspections and review activities listed in the Vulnerability Remediation project schedule(s)?

729. Has a provision been made to reassess Vulnerability Remediation project risks at various Vulnerability Remediation project stages?

730. If standardized procurement documents are needed, where can others be found?

731. Does the Vulnerability Remediation project have a formal Vulnerability Remediation project Charter?

732. How will you coordinate Procurement with aspects of the Vulnerability Remediation project?

733. If independent estimates will be needed as evaluation criteria, who will prepare them and when?

734. Have all necessary approvals been obtained?

735. Are updated Vulnerability Remediation project time & resource estimates reasonable based on the current Vulnerability Remediation project stage?

736. How will multiple providers be managed?

737. Is there a procurement management plan in place?

738. Are tasks tracked by hours?

739. Are governance roles and responsibilities documented?

740. Are milestone deliverables effectively tracked and compared to Vulnerability Remediation project plan?

741. Is it possible to track all classes of Vulnerability Remediation project work (e.g. scheduled, un-scheduled, defect repair, etc.)?

2.37 Source Selection Criteria: Vulnerability Remediation

742. Has all proposal data been loaded?

743. What documentation is necessary regarding electronic communications?

744. What does a sample rating scale look like?

745. In the technical/management area, what criteria do you use to determine the final evaluation ratings?

746. What information may not be provided?

747. What instructions should be provided regarding oral presentations?

748. Do you have designated specific forms or worksheets?

749. How do you ensure an integrated assessment of proposals?

750. What should be considered?

751. What is cost analysis and when should it be performed?

752. What aspects should the contracting officer brief the Vulnerability Remediation project on prior to evaluation of proposals?

753. How are clarifications and communications appropriately used?

754. What are the most critical evaluation criteria that prove to be tiebreakers in the evaluation of proposals?

755. What should be the contracting officers strategy?

756. Who should attend debriefings?

757. Do you prepare an independent cost estimate?

758. What procedures are followed when a contractor requires access to classified information or a significant quantity of special material/information?

759. Can you make a cost/technical tradeoff?

760. Team leads: what is your process for assigning ratings?

2.38 Stakeholder Management Plan: Vulnerability Remediation

761. Is pert / critical path or equivalent methodology being used?

762. What are the advantages and disadvantages of using external contracted resources?

763. Are mitigation strategies identified?

764. Is the performance of the supplier to be rated and documented?

765. Is Vulnerability Remediation project status reviewed with the steering and executive teams at appropriate intervals?

766. Have process improvement efforts been completed before requirements efforts begin?

767. Has the Vulnerability Remediation project manager been identified?

768. Are there processes in place to ensure internal consistency between the source code components?

769. Are risk triggers captured?

770. What information should be collected?

771. Are formal code reviews conducted?

772. Is there an issues management plan in place?

773. Are multiple estimation methods being employed?

774. Are the appropriate IT resources adequate to meet planned commitments?

775. Is the schedule updated on a periodic basis?

776. Are all payments made according to the contract(s)?

777. Are there procedures in place to effectively manage interdependencies with other Vulnerability Remediation projects / systems?

2.39 Change Management Plan: Vulnerability Remediation

778. What prerequisite knowledge do corresponding groups need?

779. How can you best frame the message so that it addresses the audiences interests?

780. What skills, education, knowledge, or work experiences should the resources have for each identified competency?

781. What relationships will change?

782. What risks may occur upfront?

783. What is the most positive interpretation it can receive?

784. Is there a software application relevant to this deliverable?

785. What is going to be done differently?

786. Who should be involved in developing a change management strategy?

787. Who is the target audience of the piece of information?

788. Do the proposed users have access to the appropriate documentation?

789. Has the relevant business unit been notified of

installation and support requirements?

790. Who is the audience for change management activities?

791. What prerequisite knowledge or training is required?

792. Will a different work structure focus people on what is important?

793. What does a resilient organization look like?

794. What do you expect the target audience to do, say, think or feel as a result of this communication?

795. Has an information & communications plan been developed?

796. What are the essentials of the message?

797. Who will do the training?

3.0 Executing Process Group: Vulnerability Remediation

798. How many different communication channels does the Vulnerability Remediation project team have?

799. It under budget or over budget?

800. Does the Vulnerability Remediation project team have enough people to execute the Vulnerability Remediation project plan?

801. When do you share the scorecard with managers?

802. Does the Vulnerability Remediation project team have the right skills?

803. What is the difference between using brainstorming and the Delphi technique for risk identification?

804. What Vulnerability Remediation projects and services are in the portfolio of your organization?

805. How could stakeholders negatively impact your Vulnerability Remediation project?

806. How well did the chosen processes fit the needs of the Vulnerability Remediation project?

807. Why should Vulnerability Remediation project managers strive to make jobs look easy?

808. In what way has the program come up with innovative measures for problem-solving?

809. Measurable - are the targets measurable?

810. Are the necessary foundations in place to ensure the sustainability of the results of the programme?

811. What is involved in the solicitation process?

812. What are crucial elements of successful Vulnerability Remediation project plan execution?

813. When will the Vulnerability Remediation project be done?

814. What is the shortest possible time it will take to complete this Vulnerability Remediation project?

3.1 Team Member Status Report: Vulnerability Remediation

815. Does the product, good, or service already exist within your organization?

816. What is to be done?

817. The problem with Reward & Recognition Programs is that the truly deserving people all too often get left out. How can you make it practical?

818. Are the attitudes of staff regarding Vulnerability Remediation project work improving?

819. Do you have an Enterprise Vulnerability Remediation project Management Office (EPMO)?

820. How will resource planning be done?

821. How can you make it practical?

822. How it is to be done?

823. What specific interest groups do you have in place?

824. Does every department have to have a Vulnerability Remediation project Manager on staff?

825. How does this product, good, or service meet the needs of the Vulnerability Remediation project and your organization as a whole?

826. Does your organization have the means (staff,

money, contract, etc.) to produce or to acquire the product, good, or service?

827. How much risk is involved?

828. When a teams productivity and success depend on collaboration and the efficient flow of information, what generally fails them?

829. Are your organizations Vulnerability Remediation projects more successful over time?

830. Is there evidence that staff is taking a more professional approach toward management of your organizations Vulnerability Remediation projects?

831. Why is it to be done?

832. Are the products of your organizations Vulnerability Remediation projects meeting customers objectives?

833. Will the staff do training or is that done by a third party?

3.2 Change Request: Vulnerability Remediation

834. How is the change documented (format, content, storage)?

835. Why do you want to have a change control system?

836. How are the measures for carrying out the change established?

837. What are the Impacts to your organization?

838. How shall the implementation of changes be recorded?

839. What are the requirements for urgent changes?

840. Will the change use memory to the extent that other functions will be not have sufficient memory to operate effectively?

841. Are there requirements attributes that are strongly related to the occurrence of defects and failures?

842. Who can suggest changes?

843. Has your address changed?

844. Who is included in the change control team?

845. How fast will change requests be approved?

846. What can be filed?

847. What must be taken into consideration when introducing change control programs?

848. How does a team identify the discrete elements of a configuration?

849. Customer acceptance plan how will the customer verify the change has been implemented successfully?

850. Who is responsible to authorize changes?

851. Are you implementing itil processes?

852. Are there requirements attributes that can discriminate between high and low reliability?

3.3 Change Log: Vulnerability Remediation

853. Do the described changes impact on the integrity or security of the system?

854. Is the submitted change a new change or a modification of a previously approved change?

855. Is the change request within Vulnerability Remediation project scope?

856. How does this change affect the timeline of the schedule?

857. Does the suggested change request seem to represent a necessary enhancement to the product?

858. When was the request approved?

859. Is the requested change request a result of changes in other Vulnerability Remediation project(s)?

860. Is this a mandatory replacement?

861. Will the Vulnerability Remediation project fail if the change request is not executed?

862. Is the change request open, closed or pending?

863. When was the request submitted?

864. Who initiated the change request?

865. Does the suggested change request represent a

desired enhancement to the products functionality?

866. How does this change affect scope?

867. Is the change backward compatible without limitations?

868. Should a more thorough impact analysis be conducted?

869. How does this relate to the standards developed for specific business processes?

870. Where do changes come from?

3.4 Decision Log: Vulnerability Remediation

871. What was the rationale for the decision?

872. How effective is maintaining the log at facilitating organizational learning?

873. Is everything working as expected?

874. How consolidated and comprehensive a story can you tell by capturing currently available incident data in a central location and through a log of key decisions during an incident?

875. Adversarial environment. is your opponent open to a non-traditional workflow, or will it likely challenge anything you do?

876. What is the average size of your matters in an applicable measurement?

877. Is your opponent open to a non-traditional workflow, or will it likely challenge anything you do?

878. What eDiscovery problem or issue did your organization set out to fix or make better?

879. What alternatives/risks were considered?

880. How does an increasing emphasis on cost containment influence the strategies and tactics used?

881. Decision-making process; how will the team

make decisions?

882. How does the use a Decision Support System influence the strategies/tactics or costs?

883. At what point in time does loss become unacceptable?

884. Who will be given a copy of this document and where will it be kept?

885. Who is the decisionmaker?

886. Behaviors; what are guidelines that the team has identified that will assist them with getting the most out of team meetings?

887. With whom was the decision shared or considered?

888. It becomes critical to track and periodically revisit both operational effectiveness; Are you noticing all that you need to, and are you interpreting what you see effectively?

889. Which variables make a critical difference?

890. How do you define success?

3.5 Quality Audit: Vulnerability Remediation

891. How does your organization know that its systems for providing high quality consultancy services to external parties are appropriately effective and constructive?

892. What are you trying to do?

893. What review processes are in place for your organizations major activities?

894. How do you indicate the extent to which your personnel would be expected to contribute to the work effort?

895. Are measuring and test equipment that have been placed out of service suitably identified and excluded from use in any device reconditioning operation?

896. How does your organization know that its information technology system is serving its needs as effectively and constructively as is appropriate?

897. Are all employees including salespersons made aware that they must report all complaints received from any source for inclusion in the complaint handling system?

898. Can your organization demonstrate exactly how and why results were achieved?

899. How does your organization know that its

staff placements are appropriately effective and constructive in relation to program-related learning outcomes?

900. How does your organization know that its management system is appropriately effective and constructive?

901. How does your organization know that the range and quality of its social and recreational services and facilities are appropriately effective and constructive in meeting the needs of staff?

902. How does your organization know that it provides a safe and healthy environment?

903. How does your organization know that its Strategic Plan is providing the best guidance for the future of your organization?

904. Have the risks associated with the intentions been identified, analyzed and appropriate responses developed?

905. How does your organization know that the system for managing its facilities is appropriately effective and constructive?

906. How does your organization know that its system for examining work done is appropriately effective and constructive?

907. What data about organizational performance is routinely collected and reported?

908. How does your organization know that its staff

embody the core knowledge, skills and characteristics for which it wishes to be recognized?

909. Are people allowed to contribute ideas?

3.6 Team Directory: Vulnerability Remediation

910. Who will talk to the customer?

911. Contract requirements complied with?

912. How and in what format should information be presented?

913. Is construction on schedule?

914. How does the team resolve conflicts and ensure tasks are completed?

915. When will you produce deliverables?

916. Process decisions: is work progressing on schedule and per contract requirements?

917. Why is the work necessary?

918. What are you going to deliver or accomplish?

919. Who will be the stakeholders on your next Vulnerability Remediation project?

920. Timing: when do the effects of communication take place?

921. Where should the information be distributed?

922. Who are your stakeholders (customers, sponsors, end users, team members)?

923. How do unidentified risks impact the outcome of the Vulnerability Remediation project?

924. Who are the Team Members?

925. Who will report Vulnerability Remediation project status to all stakeholders?

926. Who will write the meeting minutes and distribute?

927. Where will the product be used and/or delivered or built when appropriate?

928. Who should receive information (all stakeholders)?

3.7 Team Operating Agreement: Vulnerability Remediation

929. Do you ensure that all participants know how to use the required technology?

930. How do you want to be thought of and known within your organization?

931. Do you listen for voice tone and word choice to understand the meaning behind words?

932. Are there more than two functional areas represented by your team?

933. What is teaming?

934. Do you send out the agenda and meeting materials in advance?

935. Have you established procedures that team members can follow to work effectively together, such as a team operating agreement?

936. Do you solicit member feedback about meetings and what would make them better?

937. Do you post meeting notes and the recording (if used) and notify participants?

938. What is group supervision?

939. What are the safety issues/risks that need to be addressed and/or that the team needs to consider?

940. How will group handle unplanned absences?

941. Is compensation based on team and individual performance?

942. What is a Virtual Team?

943. Do you brief absent members after they view meeting notes or listen to a recording?

944. Did you determine the technology methods that best match the messages to be communicated?

945. Methodologies: how will key team processes be implemented, such as training, research, work deliverable production, review and approval processes, knowledge management, and meeting procedures?

946. What are the current caseload numbers in the unit?

947. How will you divide work equitably?

3.8 Team Performance Assessment: Vulnerability Remediation

948. If you have received criticism from reviewers that your work suffered from method variance, what was the circumstance?

949. How hard do you try to make a good selection?

950. To what degree are the goals ambitious?

951. To what degree do team members agree with the goals, relative importance, and the ways in which achievement will be measured?

952. To what degree is there a sense that only the team can succeed?

953. How much interpersonal friction is there in your team?

954. To what degree will new and supplemental skills be introduced as the need is recognized?

955. To what degree do team members understand one anothers roles and skills?

956. How hard did you try to make a good selection?

957. To what degree does the teams purpose contain themes that are particularly meaningful and memorable?

958. To what degree will the approach capitalize on and enhance the skills of all team members in a

manner that takes into consideration other demands on members of the team?

959. Individual task proficiency and team process behavior: what is important for team functioning?

960. To what degree can all members engage in open and interactive considerations?

961. When does the medium matter?

962. To what degree does the teams purpose constitute a broader, deeper aspiration than just accomplishing short-term goals?

963. To what degree can team members meet frequently enough to accomplish the teams ends?

964. What makes opportunities more or less obvious?

965. To what degree will the team ensure that all members equitably share the work essential to the success of the team?

966. Can familiarity breed backup?

967. How do you recognize and praise members for contributions?

3.9 Team Member Performance Assessment: Vulnerability Remediation

968. To what degree do team members frequently explore the teams purpose and its implications?

969. Does the rater (supervisor) have the authority or responsibility to tell an employee that the employees performance is unsatisfactory?

970. To what degree do all members feel responsible for all agreed-upon measures?

971. What resources do you need?

972. What is a significant fact or event?

973. Which training platform formats (i.e., mobile, virtual, videogame-based) were implemented in your effort(s)?

974. Where can team members go for more detailed information on performance measurement and assessment?

975. To what degree do team members feel that the purpose of the team is important, if not exciting?

976. What are the staffs preferences for training on technology-based platforms?

977. To what degree is the team cognizant of small wins to be celebrated along the way?

978. To what degree do members articulate the goals beyond the team membership?

979. How do you know that all team members are learning?

980. To what degree can the team measure progress against specific goals?

981. To what degree are the skill areas critical to team performance present?

982. Why were corresponding selected?

983. What variables that affect team members achievement are within your control?

984. Does the rater (supervisor) have to wait for the interim or final performance assessment review to tell an employee that the employees performance is unsatisfactory?

985. Goals met?

986. Are any validation activities performed?

3.10 Issue Log: Vulnerability Remediation

987. Which team member will work with each stakeholder?

988. Are there common objectives between the team and the stakeholder?

989. Are they needed?

990. How do you manage human resources?

991. Are the Vulnerability Remediation project issues uniquely identified, including to which product they refer?

992. Are stakeholder roles recognized by your organization?

993. Who do you turn to if you have questions?

994. What approaches to you feel are the best ones to use?

995. Who were proponents/opponents?

996. What is the stakeholders political influence?

997. Who reported the issue?

998. Are the stakeholders getting the information they need, are they consulted, are concerns addressed?

999. Who is the stakeholder?

1000. Which stakeholders are thought leaders, influences, or early adopters?

1001. Who have you worked with in past, similar initiatives?

1002. In your work, how much time is spent on stakeholder identification?

1003. Who is the issue assigned to?

4.0 Monitoring and Controlling Process Group: Vulnerability Remediation

1004. How are you doing?

1005. How is agile program management done?

1006. What areas does the group agree are the biggest success on the Vulnerability Remediation project?

1007. Were escalated issues resolved promptly?

1008. How well did the chosen processes fit the needs of the Vulnerability Remediation project?

1009. Did it work?

1010. How to ensure validity, quality and consistency?

1011. What will you do to minimize the impact should a risk event occur?

1012. Does the solution fit in with organizations technical architectural requirements?

1013. Just how important is your work to the overall success of the Vulnerability Remediation project?

1014. How is Agile Vulnerability Remediation project Management done?

1015. Is the program in place as intended?

1016. Change, where should you look for problems?

1017. Where is the Risk in the Vulnerability Remediation project?

1018. How many more potential communications channels were introduced by the discovery of the new stakeholders?

1019. Is it what was agreed upon?

1020. How is agile Vulnerability Remediation project management done?

1021. What were things that you did well, and could improve, and how?

4.1 Project Performance Report: Vulnerability Remediation

1022. To what degree can the cognitive capacity of individuals accommodate the flow of information?

1023. To what degree are the teams goals and objectives clear, simple, and measurable?

1024. To what degree are the structures of the formal organization consistent with the behaviors in the informal organization?

1025. To what degree does the teams work approach provide opportunity for members to engage in open interaction?

1026. To what degree are the demands of the task compatible with and converge with the relationships of the informal organization?

1027. To what degree are sub-teams possible or necessary?

1028. To what degree does the formal organization make use of individual resources and meet individual needs?

1029. To what degree can team members vigorously define the teams purpose in considerations with others who are not part of the functioning team?

1030. To what degree does the team possess adequate membership to achieve its ends?

1031. How can Vulnerability Remediation project sustainability be maintained?

1032. Next Steps?

4.2 Variance Analysis: Vulnerability Remediation

1033. Are indirect costs charged to the appropriate indirect pools and incurring organization?

1034. Are there changes in the overhead pool and/or organization structures?

1035. How have the setting and use of standards changed over time?

1036. What is your organizations rationale for sharing expenses and services between business segments?

1037. What business event caused the fluctuation?

1038. How are variances affected by multiple material and labor categories?

1039. Wbs elements contractually specified for reporting of status to your organization (lowest level only)?

1040. Are the bases and rates for allocating costs from each indirect pool consistently applied?

1041. What is the performance to date and material commitment?

1042. How are material, labor, and overhead standards set?

1043. Do work packages consist of discrete tasks which are adequately described?

1044. Are all cwbs elements specified for external reporting?

1045. Contemplated overhead expenditure for each period based on the best information currently is available?

1046. How does the use of a single conversion element (rather than the traditional labor and overhead elements) affect standard costing?

1047. Who are responsible for the establishment of budgets and assignment of resources for overhead performance?

1048. Contract line items and end items?

1049. What is the actual cost of work performed?

1050. Who is generally responsible for monitoring and taking action on variances?

1051. Are your organizations and items of cost assigned to each pool identified?

4.3 Earned Value Status: Vulnerability Remediation

1052. Where is evidence-based earned value in your organization reported?

1053. Where are your problem areas?

1054. Are you hitting your Vulnerability Remediation projects targets?

1055. Verification is a process of ensuring that the developed system satisfies the stakeholders agreements and specifications; Are you building the product right? What do you verify?

1056. When is it going to finish?

1057. What is the unit of forecast value?

1058. How does this compare with other Vulnerability Remediation projects?

1059. If earned value management (EVM) is so good in determining the true status of a Vulnerability Remediation project and Vulnerability Remediation project its completion, why is it that hardly any one uses it in information systems related Vulnerability Remediation projects?

1060. Earned value can be used in almost any Vulnerability Remediation project situation and in almost any Vulnerability Remediation project environment. it may be used on large Vulnerability Remediation projects, medium sized Vulnerability

Remediation projects, tiny Vulnerability Remediation projects (in cut-down form), complex and simple Vulnerability Remediation projects and in any market sector. some people, of course, know all about earned value, they have used it for years - but perhaps not as effectively as they could have?

1061. How much is it going to cost by the finish?

1062. Validation is a process of ensuring that the developed system will actually achieve the stakeholders desired outcomes; Are you building the right product? What do you validate?

4.4 Risk Audit: Vulnerability Remediation

1063. Is the customer technically sophisticated in the product area?

1064. Does the customer understand the process?

1065. Is the auditor truly independent?

1066. Are all financial transactions accurately recorded (receipted, banked)?

1067. What does monitoring consist of?

1068. Do requirements put excessive performance constraints on the product?

1069. Are some people working on multiple Vulnerability Remediation projects?

1070. Does your organization have a register of insurance policies detailing all current insurance policies?

1071. Have all possible risks/hazards been identified (including injury to staff, damage to equipment, impact on others in the community)?

1072. How will you maximise opportunities?

1073. To what extent are auditors influenced by the business risk assessment in the audit process, and how can auditors create more effective mental models to more fully examine contradictory

evidence?

1074. What is the anticipated volatility of the requirements?

1075. Where will the next scandal or adverse media involving your organization come from?

1076. Do you have position descriptions for all office bearers/staff?

1077. Do requirements demand the use of new analysis, design, or testing methods?

1078. Is safety information provided to all involved?

1079. How do you govern assets?

1080. If applicable; are compilers and code generators available and suitable for the product to be built?

4.5 Contractor Status Report: Vulnerability Remediation

1081. What was the actual budget or estimated cost for your organizations services?

1082. How long have you been using the services?

1083. What are the minimum and optimal bandwidth requirements for the proposed solution?

1084. Are there contractual transfer concerns?

1085. What was the budget or estimated cost for your organizations services?

1086. If applicable; describe your standard schedule for new software version releases. Are new software version releases included in the standard maintenance plan?

1087. How is risk transferred?

1088. What was the final actual cost?

1089. Who can list a Vulnerability Remediation project as organization experience, your organization or a previous employee of your organization?

1090. What process manages the contracts?

1091. Describe how often regular updates are made to the proposed solution. Are corresponding regular updates included in the standard maintenance plan?

1092. What was the overall budget or estimated cost?

1093. What is the average response time for answering a support call?

4.6 Formal Acceptance: Vulnerability Remediation

1094. Does it do what Vulnerability Remediation project team said it would?

1095. Do you perform formal acceptance or burn-in tests?

1096. Have all comments been addressed?

1097. What features, practices, and processes proved to be strengths or weaknesses?

1098. What is the Acceptance Management Process?

1099. What function(s) does it fill or meet?

1100. Do you buy-in installation services?

1101. Was the sponsor/customer satisfied?

1102. How does your team plan to obtain formal acceptance on your Vulnerability Remediation project?

1103. Who supplies data?

1104. What lessons were learned about your Vulnerability Remediation project management methodology?

1105. General estimate of the costs and times to complete the Vulnerability Remediation project?

1106. Who would use it?

1107. Was the Vulnerability Remediation project goal achieved?

1108. Was the Vulnerability Remediation project work done on time, within budget, and according to specification?

1109. Was the Vulnerability Remediation project managed well?

1110. What are the requirements against which to test, Who will execute?

1111. Did the Vulnerability Remediation project achieve its MOV?

1112. Was the client satisfied with the Vulnerability Remediation project results?

1113. Do you buy pre-configured systems or build your own configuration?

5.0 Closing Process Group: Vulnerability Remediation

1114. What areas were overlooked on this Vulnerability Remediation project?

1115. Based on your Vulnerability Remediation project communication management plan, what worked well?

1116. What is the Vulnerability Remediation project Management Process?

1117. Are there funding or time constraints?

1118. Did the Vulnerability Remediation project team have the right skills?

1119. Were risks identified and mitigated?

1120. Were sponsors and decision makers available when needed outside regularly scheduled meetings?

1121. How dependent is the Vulnerability Remediation project on other Vulnerability Remediation projects or work efforts?

1122. What is the risk of failure to your organization?

1123. What is the amount of funding and what Vulnerability Remediation project phases are funded?

1124. How critical is the Vulnerability Remediation project success to the success of your organization?

1125. What communication items need improvement?

1126. Did the Vulnerability Remediation project team have enough people to execute the Vulnerability Remediation project plan?

1127. What could have been improved?

1128. How will you do it?

1129. Is the Vulnerability Remediation project funded?

1130. Mitigate. what will you do to minimize the impact should a risk event occur?

5.1 Procurement Audit: Vulnerability Remediation

1131. Is an appropriated degree of standardization of goods and services respected?

1132. Are the purchase order forms designed for efficient and simple completion?

1133. Was the formal review of requests to participate or evaluation of bids correctly undertaken?

1134. Does the department have a procurement strategy and is it implemented?

1135. Are there systems for recording and monitoring in order to discover malpractice and fraud in the procurement function/unit?

1136. Are staff members evaluated in accordance with the terms of existing negotiated agreements?

1137. Are there procedures for trade-in arrangements?

1138. Is the procurement process fully digitalized?

1139. Does procurement staff have recognized professional procurement qualifications or sufficient training?

1140. Has the award included no items different from the already stated contained in bid specifications?

1141. Who are the key suppliers?

1142. Is there management monitoring of transactions and balances?

1143. How do you monitor behaviour of procurement staff?

1144. Was the payment made to the supplier/ contractor within the time frames indicated in the contracts?

1145. Does the cash disbursement policy prohibit drawing checks to cash or bearer?

1146. Were results of the award procedures published?

1147. Are cases of double payment duly prevented and corrected?

1148. Was the estimation of contract value in accordance with the criteria fixed in the Directive?

1149. Are procedures established so that vendors with poor quality or late delivery are identified to eliminate additional dealings with that vendor?

1150. Is the approval graduated according to the amount disbursed?

5.2 Contract Close-Out: Vulnerability Remediation

1151. How does it work?

1152. How/when used ?

1153. Parties: who is involved?

1154. Have all contract records been included in the Vulnerability Remediation project archives?

1155. Was the contract type appropriate?

1156. Are the signers the authorized officials?

1157. Have all acceptance criteria been met prior to final payment to contractors?

1158. Parties: Authorized?

1159. What happens to the recipient of services?

1160. Was the contract sufficiently clear so as not to result in numerous disputes and misunderstandings?

1161. Change in attitude or behavior?

1162. How is the contracting office notified of the automatic contract close-out?

1163. Was the contract complete without requiring numerous changes and revisions?

1164. Change in circumstances?

1165. Have all contracts been closed?

1166. What is capture management?

1167. Have all contracts been completed?

1168. Change in knowledge?

1169. Has each contract been audited to verify acceptance and delivery?

5.3 Project or Phase Close-Out: Vulnerability Remediation

1170. What information is each stakeholder group interested in?

1171. What security considerations needed to be addressed during the procurement life cycle?

1172. Who are the Vulnerability Remediation project stakeholders and what are roles and involvement?

1173. What was the preferred delivery mechanism?

1174. What were the actual outcomes?

1175. In addition to assessing whether the Vulnerability Remediation project was successful, it is equally critical to analyze why it was or was not fully successful. Are you including this?

1176. Is there a clear cause and effect between the activity and the lesson learned?

1177. What was learned?

1178. What advantages do the an individual interview have over a group meeting, and vice-versa?

1179. Who controlled key decisions that were made?

1180. Planned completion date?

1181. Have business partners been involved extensively, and what data was required for them?

1182. Planned remaining costs?

1183. What are the mandatory communication needs for each stakeholder?

1184. Was the schedule met?

1185. Complete yes or no?

1186. How often did each stakeholder need an update?

5.4 Lessons Learned: Vulnerability Remediation

1187. How well does the product or service the Vulnerability Remediation project produced meet the defined Vulnerability Remediation project requirements?

1188. How useful do individuals find communications?

1189. How well do you feel the executives supported this Vulnerability Remediation project?

1190. How smooth do you feel Integration has been?

1191. What mistakes did you successfully avoid making?

1192. What were the problems encountered in the Vulnerability Remediation project-functional area relationship, why, and how could they be fixed?

1193. What other questions should you have asked?

1194. What is the supervisor to staff ratio?

1195. Was the control overhead justified?

1196. What is the frequency of personal communications?

1197. What is the impact of tax policy?

1198. How timely were Progress Reports provided to

the Vulnerability Remediation project Manager by Team Members?

1199. How well were your expectations met regarding the extent of your involvement in the Vulnerability Remediation project (effort, time commitments, etc.)?

1200. What worked well or did not work well, either for this Vulnerability Remediation project or for the Vulnerability Remediation project team?

1201. How was the Vulnerability Remediation project controlled?

1202. Was the change control process properly implemented to manage changes to cost, scope, schedule, or quality?

1203. Did the Vulnerability Remediation project improve the team members reputations, skills, personal development?

1204. What skills did you need that were missing on this Vulnerability Remediation project?

1205. What is the fiscal dependency?

Index

ability 40, 51, 115
absences 249
absent 249
absolute 33, 80
accept 74, 88, 216
acceptable 131
acceptance 6, 238, 268, 274-275
accepted 101, 155, 199
access 4, 9-10, 26, 50, 57, 61, 63, 91, 95-96, 112, 116, 118, 120, 124, 128-129, 138, 174, 193, 199, 228, 231
accessed 57, 139
accesses 36
accomplish 8, 148, 158, 178, 207, 246, 251
accordance 272-273
according 30, 32, 230, 269, 273
account 31, 173, 187, 217
accounted 47, 129
accounts 108, 208
accuracy 50, 166
accurate 10, 174, 179, 191
accurately 264
achieve 8, 120, 178, 205, 223, 258, 263, 269
achieved 25, 243, 269
achieving 44, 153
acquire 236
acquired 121, 177, 205
across 76, 108, 110, 121, 143
action 105, 167, 218, 261
actionable 62
actioned 211
actions 45, 89, 102, 154, 209
active 51
activities 40, 44-45, 83, 89, 96, 110, 174-179, 181-183, 185, 189, 191-192, 194-196, 215, 225, 232, 243, 253
activity 5, 32, 38, 102, 153, 172, 176-178, 180-181, 183-184, 187-188, 191, 195, 276
actual 38, 106, 171, 188, 195, 261, 266, 276
actually 30, 73, 77, 100, 120, 203, 263
actuals 194
adaptation 23

adapting 87
addition 210, 276
additional 39, 59, 62, 64, 66, 100, 111, 197, 217, 273
additions 90
address 1, 21, 32, 71, 129, 138, 158, 174, 237
addressed 184, 248, 254, 268, 276
addresses 231
addressing 40, 71, 107, 140
adequate 48, 138, 167, 172, 230, 258
adequately 39, 260
adherence 140
adopters 255
adoption 124
advance 217, 248
advantage 1, 204
advantages 61-62, 112, 162, 229, 276
adverse 265
advertise 107
advise 2
affect 88, 118, 128, 143, 151, 153, 163, 188, 195, 200, 218, 220, 239-240, 253, 261
affected 101, 126, 151, 193, 211, 260
affecting 12
afford 215
afraid 207
against36, 85, 87, 92, 95-96, 194, 200, 253, 269
agencies 151
agenda 248
agents 114
aggregate 77
agreed 46, 96, 160, 193, 211-212, 257
agreement 6, 139, 160, 248
agreements 34, 262, 272
agrees 206
alerted76
alerting 79, 160
alerts 72
algorithms 137, 220
aligned 23, 56, 116
aligning 87
Alignment 153, 212
alleged 3
allocated 195, 207

allocating 172, 260
allocation 172
allowance 106
allowed 2, 108, 185, 245
allows 10
almost 262
already 102, 138, 171, 201, 203, 235, 272
altogether 219
always 10, 115, 131, 195
ambitious 250
amount 24, 63, 138, 270, 273
amplify 58
amputation 71
analysis 4, 6, 10-11, 43, 46-50, 55-56, 60, 64, 66, 70-71, 79, 151, 155, 160, 175, 198-199, 219, 221, 223, 227, 240, 260, 265
analyst 45
analyze 4, 44, 54, 57, 59, 77, 194, 203, 276
analyzed 45, 75, 157, 160, 165, 244
announced 122
annual 64
another 113, 169, 179, 220
anothers 250
answer 11-12, 18, 29, 43, 54, 69, 85, 100
answered 26, 40, 52, 67, 83, 98, 144
answering 11, 180, 267
anybody 102
anyone 31
anything 51, 132, 176, 184, 195, 200, 241
appear 3, 216
applicable 11, 161, 192, 241, 265-266
applied 46, 107, 153, 155, 217, 260
applying 121, 135
appointed 29, 39
appreciate 209
approach 174, 225, 236, 250, 258
approaches 21, 50, 254
approval 74, 249, 273
approvals 225
approve 165
approved 20, 91, 131, 141, 155, 163, 174, 200, 212, 237, 239
approver 88
approving 163
architect 78

Architects 8
archived 193, 200, 225
archives 274
arthritis 80
articulate 253
asking 3, 8, 199, 205
aspect 214
aspects 59-60, 180, 225, 227
aspiration 251
assess 77, 182
assessed 49, 55, 80, 142, 211
assessing 86, 276
assessment 6, 9-10, 22, 58, 63, 65, 75, 77, 82, 96, 101, 103, 107, 118, 123, 130, 132, 142, 175, 194, 209, 219, 227, 250, 252-253, 264
assets 19, 56, 65, 107, 141-143, 265
assign 117
assigned 30, 38, 91, 103, 116, 158, 165, 169, 174, 178, 255, 261
assigning 228
assignment 5, 179, 207, 261
assist 9, 48, 70, 97, 188, 198, 242
assistance 25
assistant 8
associated 60, 80, 112, 122, 161, 244
assume 217
assuming 219
Assumption 4, 70, 167
assurance 44, 79, 83, 96, 112, 157
assure 50, 61
attached 189
attack 80, 90, 109-110, 121-122, 133
attacked 123
attacker 112, 117, 120, 135
attackers 82
attacks18, 134
attainable 39
attempted 31
attempts 109, 116
attend 228
attendance 39
attendant 82
attended 1, 40

attention 12, 141
attitude 274
attitudes 235
attributes 5, 161, 175, 178, 237-238
audience 231-232
audiences 202, 231
audited 90, 125, 129, 275
auditing 79, 86, 167
auditor 264
auditors 264
audits 91, 95, 201
author 3
authority 159-160, 210, 213, 252
authorize 238
authorized 171-172, 274
automated 19, 50
automatic 274
automation 80, 92
available 18, 25, 38-39, 75, 80, 88, 92, 107, 110-111, 146, 171, 176-177, 186-187, 192, 202, 215-216, 221-223, 241, 261, 265, 270
average 12, 26, 40, 52, 63, 67, 72, 77, 83, 98, 123, 130, 144, 189, 241, 267
averse 215
awareness 106, 114, 181
background 10
backup 61, 63, 135, 251
backward 240
balance 81
balances 273
bandwidth 266
banked 264
barriers 113, 214
baseline 5, 51, 70, 72, 90, 126, 133, 158, 160, 174, 199
baselined 49
baselines 81, 200
bearer 273
bearers 265
because 2, 191
become 136, 163, 242
becomes 220, 242
before 1-2, 10, 31, 56, 128, 135, 140, 165, 200, 221, 229
beginning 4, 17, 20, 26, 41, 52, 67, 83, 98, 144

behavior 25, 77, 113, 251, 274
behaviors 26, 242, 258
behaviour 273
behind 2, 119, 123, 248
belief 11, 18, 29, 43, 54, 69, 85, 100
believe 2, 105
beneficial 203
benefit 3, 19, 24-25, 79, 88, 151, 188, 217
benefits 25, 65-66, 100, 161
better 8, 34, 49, 58, 61, 104, 189, 197, 223, 241, 248
between 45, 54, 60, 90, 103, 108, 131, 133, 163, 167-168, 201, 214, 229, 233, 238, 254, 260, 276
beyond 253
bidding 195
biggest 113, 203, 225, 256
bottleneck 176
boundaries 35, 48
bounds 35
breach 44, 61
breached 75
breaches 47, 64
Breakdown 5, 72, 169, 185
breaking 123
briefed 29, 115
brings 30
broader 251
broken 61
brought 143
budding 115
budget 2, 72, 171-172, 176, 190, 192, 233, 266-267, 269
budgets 172, 208, 261
buffer 141
building 262-263
bureau 127
burn-in 268
business 2, 8, 10, 38, 44, 46-47, 54, 56, 59, 71, 74, 81-82, 87, 93, 95, 116, 122, 125, 129-130, 132, 134, 136-137, 141, 143, 147, 151, 160-161, 174, 199, 203, 208, 216, 231, 240, 260, 264, 276
busywork 147
buy-in 268
calculate 181-182, 187
cannot 24, 182
capability 46, 132, 194, 199

capable 8, 32, 207
capacity 24, 94, 258
capitalize 250
capture 88, 127, 203, 275
captured 94, 157, 174, 193, 211, 229
capturing 241
career 163, 187
carried 43, 223
carrying 237
caseload 249
catalogue 141
catching 1
categories 107, 260
category 171
caught 70
caused 3, 44, 90, 260
causes 48, 54, 62, 65, 89, 156
causing 21
celebrate 22
celebrated 252
centers 57
central 241
centrally 95
certain 57, 62, 80, 88, 103, 143
certified 193
challenge 8, 241
champion 37
change 6, 18, 25, 31, 44, 50, 57, 92, 103, 110, 115, 143, 149-150, 156, 159-160, 165, 169, 178, 182, 196, 200, 218, 221, 231-232, 237-240, 257, 274-275, 279
changed 31, 66, 109, 158, 161, 197, 199, 221, 237, 260
changes 20-21, 46, 82, 87, 90, 120, 136, 141, 155, 159, 161, 167, 171-172, 188, 193, 200, 209, 211, 237-240, 260, 274, 279
channel 63
channels 162, 233, 257
character 126
charge 62
charged 260
Charter 4, 33, 39, 148-149, 225
charters 38
charting 175
charts 44, 51, 60, 191
checked 93-94, 97, 101, 162

checklists 9, 194, 212
checks 55-56, 63, 112, 273
choice 248
choose 11, 77
chosen 114, 149, 154, 223, 233, 256
circumvent 20
claimed 3
classes 193, 226
classified 59, 228
clearly 11, 18, 29, 37, 43, 54, 69, 72, 80, 85, 100, 161-162, 171, 174, 194, 210
clickety 123
client 107, 156, 223, 269
climate 23
closed 95, 239, 275
closely 10, 123
Close-Out 6-7, 274, 276
Closing 6, 66, 270
clouds 33
Coaches 29-30, 143
coding 92, 106, 133, 167
cognitive 258
cognizant 252
colleagues 190
collect 91, 197
collected 34, 44, 49, 60, 62, 75, 165, 229, 244
collecting 96
collection 45, 47-49, 51, 55, 59-60, 205
collector 54-56, 62, 64-66
commands 61, 113
comments 268
commercial 133
commitment 151, 205, 260
committed 35, 71, 219, 222
Committee 211
common 103, 119, 148, 174, 193, 195, 254
community 23, 159, 189-190, 197-198, 201, 264
companies 3, 102, 125, 188
company 1-2, 8
comparable 155
compare 102, 120, 217, 262
compared 126, 142, 188, 194, 220, 226
comparing 155

comparison 11, 136
compatible 240, 258
compelling 32
competency 231
competitor 2
compile 201
compiler 124
compilers 222, 265
complain 203
complaint 64, 243
complaints 243
complete 3, 9, 11, 40, 104, 166, 176, 182, 189, 215, 234, 268, 274, 277
completed 12, 31, 34, 36, 38, 165-166, 188, 229, 246, 275
completely 1, 117
completing 169, 182
completion 32, 173, 262, 272, 276
complex 8, 138, 142, 263
compliance 1, 20, 30, 32, 34, 37, 48, 55, 73, 90-91, 96-97, 101, 106, 110, 114-115, 121, 123, 137-139, 149, 168
complied 246
component 46
components 44, 51, 56-57, 125-126, 129, 137, 141, 225, 229
compute 12
concept 166, 205
concerned 20
concerning 127
concerns 2, 22, 254, 266
condition 94, 154, 192
conditions 72, 94, 156
conduct 96, 108
conducted 69, 132, 137, 175, 193-194, 229, 240
conducting 141
confidence 182
confident 182
configure 126
configured 22, 134
confirm 11
conflict101, 160, 222
conflicts 203, 246
connected 191
connecting 33
connection 33

consent 55
consider 20, 71-72, 74, 88-89, 96, 101, 133, 178, 188, 248
considered 21, 32, 79, 227, 241-242
consist 260, 264
consistent 57, 59-60, 63, 92, 108, 154-155, 196, 258
console 111
consortium 221
constantly 1
constitute 251
Constraint 4, 167
consult 1, 87, 137
consultant 1-2, 8
consulted 254
consulting 2
contact 8, 20, 202
contain 23, 95, 102, 130, 250
contained 3, 272
container 77
contains 9
content 31, 34, 237
contents 3-4, 9
context 76, 187
continual 89, 95
Continuity 180
continuous 97
contract 6, 62, 92, 171-172, 193, 195, 208, 230, 236, 246, 261, 273-275
contracted 229
contractor 6, 159, 172, 228, 266, 273
contracts 91, 113, 172, 187, 194, 266, 273, 275
contribute 154, 243, 245
control 4, 55, 72, 74, 77, 85, 89, 91, 95-97, 151, 159, 171, 173-174, 198, 207-208, 237-238, 253, 278-279
controlled 95, 157, 172, 208, 276, 279
controls 23, 66, 76, 86-87, 90, 94-95, 97, 183, 217
convenient 121
converge 258
conversion 261
convey 3
cooperate 197
coordinate 225
Copyright 3
corporate 2, 33, 55, 82

correct 43, 85, 111, 191, 194
corrected 273
corrective 89, 217
correctly 22, 272
correspond 9-10
corrupted 64
costing 196, 261
course 31, 263
coverage 121
covering 9, 210
create 21, 25, 115, 202, 264
created 58, 150, 187, 212, 223
creating 8, 154
creation 220
creativity 78
credible 197
crisis 19, 109, 126
criteria 4, 6, 9-10, 39, 44, 57, 70, 72, 77, 80, 145, 163, 175, 198-199, 225, 227-228, 273-274
CRITERION 4, 18, 29, 43, 54, 69, 85, 100
critical 31, 34, 39, 46, 56, 58-59, 63, 71, 87, 91, 101, 115, 131, 153-154, 176, 228-229, 242, 253, 270, 276
criticism 250
crucial 63, 81, 180, 207, 234
crypto 101
crystal 11
cultural 80
culture 55, 121, 204, 209
current 30, 43-45, 60-62, 66, 112-113, 132, 158, 161, 172, 188, 193, 201, 210, 217-219, 226, 249, 264
currently 30, 55, 119, 171, 241, 261
custom 126
customer 21, 32, 34-36, 92-93, 161, 199, 201-202, 215, 219, 221-222, 238, 246, 264, 268
customers 3, 19, 36-37, 40, 64, 148, 212, 215, 223, 236, 246
customized 2
cut-down 263
damage 3, 264
Dashboard 9
dashboards 90
database 58-59, 63
data-level 50
day-to-day 89

deadline 50
dealer 193
dealings 273
decide 126, 187, 201
decision 6, 210, 241-242, 270
decisions 24, 193, 195, 241-242, 246, 276
declining 136
decrease 123
decreases 140
decreasing 106
dedicated 8, 109, 132
deemed 101
deeper 11, 251
default 137
defect 46, 193, 203, 226
defects 46, 110, 121, 134, 237
define 4, 29, 31, 33, 48, 52, 148, 188, 242, 258
defined 11, 18, 23, 29, 37, 39-40, 43, 46, 54, 69, 72, 80, 85, 100, 153, 157-158, 165, 167, 169, 171-172, 174-175, 178, 194, 204, 210, 278
defines 39, 185-186, 195
defining 8, 149, 167, 174
definite 95, 178
definition 157, 167, 187, 193, 215
degree 250-253, 258, 272
-degree 2
delayed 181
delays 176, 189
delegated 32
deletions 90
deliver 19, 39, 197, 246
delivered 33, 89, 104, 124, 185, 199, 247
delivering 122
delivers 185
delivery 181-182, 273, 275-276
Delphi 233
demand 219, 265
demands 251, 258
democratic 76
denial 51
department 8, 25, 235, 272
departure 121
depend 236

dependency 279
dependent 270
depending 64
deployed 45, 91
deployment 65, 78
deprived 138
Describe 69, 160, 163, 180, 266
described 3, 173-174, 200, 239, 260
describing 36
deserving 235
design 10, 44, 48-50, 69-70, 75, 79, 81, 95, 103, 167-168, 221, 265
designated 227
designed 8, 10, 63-64, 78, 82, 86, 125, 142, 272
designing 8
designs 80, 85
desired26, 39, 186, 240, 263
desktop 94, 114
destroy56
detail 148, 165, 169, 189
detailed 49-50, 58-59, 96, 157, 172-173, 252
detailing 264
detect 63, 94, 110, 120, 122
detecting 143
detection 49
determine 10, 40, 45, 105, 176, 187-188, 197, 212, 227, 249
determined 58, 148, 205
develop 24, 69, 81, 155, 169
developed 10, 33, 37-38, 70, 73, 155, 157, 167-168, 177, 200, 205, 232, 240, 244, 262-263
developer 76
developers 72, 86, 215
developing 59, 71, 207, 231
device 243
devices 19, 36, 50, 96, 137
devotes 138
diagram 5, 54, 182
diagrams 175
dialogue 76
dictates 191
Dictionary 5, 171, 173
differ 64-65, 130, 192
difference 90, 108, 154, 233, 242

different 8, 19, 30-32, 37, 54, 58, 62, 65, 80, 101, 134, 143, 149, 168, 202, 210, 232-233, 272
difficult 113, 117, 131, 176, 181, 185, 199
digital 133
diligence 82
direct 71, 172, 208
direction 31, 156
Directive 273
directly 3, 136, 151, 213
Directory 6, 46, 246
disabled 124
disabling 71
Disagree 11, 18, 29, 43, 54, 69, 85, 100
disbursed 273
disclose 110
disclosed 24, 58, 106, 110
disclosure 113, 121, 128
disconnect 86
discover 272
discovered 24, 77, 109, 114, 127, 135
discovery 78, 110, 257
discrete 238, 260
display 51
displayed 34, 43-44, 49, 61, 189
disposed 200
disputes 274
disruption 43
distribute 113, 247
divergent 154
diverse 62
divide 249
Divided 26, 32, 40, 52, 67, 83, 98, 144
division 157
document 10, 33, 55, 70-71, 80, 82, 159, 161, 165, 167-168, 174, 242
documented 35, 56, 72, 90, 93, 95, 97, 147, 153, 166, 168, 172, 175, 200, 209, 212, 226, 229, 237
documents 8, 168, 193, 225
dollars 112, 208
domain 127
domains 122
double 273
downtime 44

drawing 113, 273
driven 65
duplicates 160
duration 5, 153-154, 172, 187, 189, 219
durations 38, 191
during 20, 31, 66, 73, 78, 80, 109, 113, 129, 178, 184, 194-195, 203, 219, 221-222, 241, 276
dynamics 36
eagerly 2
earlier 171
earned 6, 262-263
economical 156
economy 188
ecosystem 107
eDiscovery 241
edition 9
editorial 3
educated 1
education 93, 231
effect 218, 276
effective 21, 33, 55, 76, 82, 102, 129, 138, 143, 189, 241, 243-244, 264
effects 71, 180, 213, 246
efficient 211, 236, 272
effort 26, 32, 225, 243, 252, 279
efforts 31, 47, 202, 229, 270
either 137, 178, 279
Electrical 168
electronic 3, 138, 227
element 261
elements 10, 44, 165-166, 171, 207-208, 234, 238, 260-261
eliminate 273
eliminated 202, 208
e-mail 162
emails 122
embarking 32
embedded 135
embody 245
emerge 25
emerging 1, 93
emphasis 241
employ 114
employed 230

employee 113, 124, 252-253, 266
employees 18, 24-26, 62, 91, 96, 102, 106, 112, 117, 121, 125, 130, 134, 201-202, 243, 252-253
employer 130
employers 150
empower 8, 93
enable 55
encourage 78
encrypted 63
endpoint 131
endpoints 86
energy 1
engage 251, 258
engaged 71
engagement 31, 86-90, 92-93, 96-97, 108, 114, 124, 137, 150, 214
Engineers 168
enhance 250
enhancing 87
enough 8, 20, 108, 146, 163, 174, 221, 233, 251, 271
ensure 36, 38, 72, 82, 90, 94, 112, 130, 137, 139-140, 149, 201, 205, 210-211, 227, 229, 234, 246, 248, 251, 256
ensuring 10, 262-263
enterprise 77, 110, 114, 235
entire 110, 208
entirety 32
entity 3
equally 276
equipment 146, 243, 264
equipped 38, 49
equitably 32, 130, 249, 251
equivalent 229
errors 118, 195
escalated 256
Escalation 56, 199
essential 196, 251
essentials 232
establish 69, 109, 198
estimate 155, 189, 195, 228, 268
estimated 32, 155, 197, 217, 266-267
estimates 5, 30, 63, 155, 157-158, 171, 187, 193-195, 200, 225-226
Estimating 5, 157, 189, 193, 197

estimation 119, 153, 212, 230, 273
estimator 195
ethics 108
evaluate 46, 60, 70, 75, 79-80, 174
evaluated 200, 272
evaluating 70
evaluation 86, 96, 172, 225, 227-228, 272
events 19, 79, 148, 173, 187
Everyday 1
everyone 32, 36, 204, 206
everything 241
evidence 11, 91, 217, 236, 265
evident 201
evolution 43
evolved 60, 129
exactly 118, 130, 209, 243
examine 264
examining 244
Example 4, 9, 13, 156, 168
examples 8-9, 153
excellence 8
exception 56, 115
exceptions 74
excess 172
excessive 264
excited 1
exciting 252
excluded 243
execute 140, 146, 233, 269, 271
executed 48-49, 200, 239
Executing 6, 114, 233
execution 168, 234
executive 8, 158, 229
executives 278
existence 224
existing 10, 21, 80, 156, 272
expect 110, 114, 159, 189, 232
expected 25, 38, 50, 75, 156, 188, 202, 241, 243
expense 208
expenses 260
expensive 101
experience 141, 190, 207, 266
expertise 26

experts 31, 207
expiration 139
explained 10
exploit 26, 33, 117, 124, 131, 134
exploited 77, 79, 103, 115, 120
exploits 122
explore 54, 252
explored 219
export 151
exposed 63
exposure 66, 115
express 66
extensive 2
extent 11, 20, 22, 24, 34, 44, 88, 153-154, 208, 237, 243, 264, 279
external 1-2, 31, 74, 103, 207, 213, 229, 243, 261
externally 61, 111
facilitate 11, 90
facilities 57, 124, 244
facility 102
facing 20, 23, 71, 111
factor 118
factors 52, 56, 61, 148, 182, 198
failed 116
failure 151, 270
failures 237
fairly 32
familiar 9, 140
fashion 3, 38
fatigue 138
faults 120
feasible 198
feature 10
features 111, 155, 268
FedRAMP 60, 90
feedback 34, 36, 40, 248
feeling 1
figure 46
Filter 203
finalized 13
financial 61, 63, 65, 93, 264
finding 102
findings 55
fingertips 10

finish 148, 180, 183, 262-263
finished 158
fiscal 279
fixing 134
flexible 21
focused 21
folder 46
follow 60, 90, 154, 183, 188, 248
followed 30, 157, 167, 171, 194, 212, 228
following 9, 11, 201
follow-up 195
forced 26, 112
forces 136
forecast 262
forget 10
forgotten 221
formal 6, 66, 103, 158, 160, 225, 229, 258, 268, 272
formally 59, 157, 172, 199, 222
format 10, 237, 246
formats 215, 252
formed30, 35
formula 12
Formulate 29
forward 2
foster 217
fourth 114
frames 187, 273
framework 206
frameworks 95
frequency 86, 205, 278
frequent 165-166
frequently 106, 113, 251-252
friction 250
friends 2
fulfil 34
full-scale 79
function 110, 142, 268, 272
functional 111, 156, 194, 248
functions 62-63, 143, 158, 161, 165, 185, 237
funded128, 270-271
funding 217, 270
further 9, 75, 103
future 8, 49, 73, 94, 96, 153, 156, 218-220, 244

gained 2, 59, 89, 93
gather 11, 43, 201
gathered 160
gathering 133, 161
General 178, 268
generally 236, 261
generate 30, 62, 64, 70
generated 36, 59, 80, 101
generation 9
generators 222, 265
generic 2
getting 2, 22, 70, 73, 125, 138, 242, 254
govern 265
governance 55, 66, 125, 153, 212, 226
gracefully 125
graduated 273
granted 199
graphical 191
graphs 9, 44
greater 108, 153, 156
greatest 65, 118
grievance 64, 113, 142
ground 48, 65
grouped 178
groups 44, 113, 116, 185, 193, 211, 231, 235
growth 180
guaranteed 33
guidance 37, 79, 107, 244
guidelines 139, 242
hacked 130
hackers 22
handle 20, 60, 133, 142, 184, 207, 222, 224, 249
handling 56, 63, 128, 142, 243
happen 26, 181, 223
happens 8, 135, 140, 198, 217, 223, 274
hardening 110, 143
hardly 262
hardware 112
hashing 126
Having 97, 218
hazards 223, 264
health 111
healthy 244

helpful 51
helping 8, 148
higher 65, 138, 203
highest 24
high-level 31, 34, 148
highlight 2, 119, 209, 217
highly 122
hiring 90
historical 198
history 176
hitters 60
hitting 262
holiday 2
Honestly 2
hosted 114
hotline 94
humans 8
hygiene 138
hypotheses 54
iDefence 135
identified 3, 23, 25, 32, 35, 40, 46, 48-49, 51, 55, 60, 66, 153, 157, 161, 167, 171, 175, 178, 200, 208-209, 211, 217-218, 223, 229, 231, 242-244, 254, 261, 264, 270, 273
identify 1, 10-11, 18, 22, 54, 56, 76, 95, 152, 197, 238
images 77
imbedded 93
immediate 48
impact 6, 34, 40, 44-47, 50, 74, 87, 161, 200, 217, 219-221, 233, 239-240, 247, 256, 264, 271, 278
impacted 46, 51
impacts 45, 49, 51, 97, 152, 154, 190, 237
impetus 119
implement 38, 45, 76, 85, 95, 110, 115, 123
import 151
importance 250
important 21, 51, 101, 105, 109, 111, 115, 117, 119, 127, 129, 138, 140, 147, 152, 157, 188, 203, 214, 232, 251-252, 256
improve 4, 10, 56, 69, 76, 78, 87, 167, 186, 203-204, 257, 279
improved 2, 71, 73, 76, 88, 153, 271
improving 235
inaccurate 135
inadequate 1

incentives 90
incidence 222
incident 49, 56, 63, 86, 126, 128, 132, 142, 241
incidents 20, 113
include 93, 96, 113, 125, 135, 155, 177
included 4, 9, 21, 103, 107, 161, 189, 195, 197, 237, 266, 272, 274
includes 10, 47, 157
including 29, 36, 39, 72, 167, 171, 175, 243, 254, 264, 276
inclusion 243
incomplete 135
increase 22, 221
increased 210
increasing 241
incurring 172, 260
in-depth 9, 11
indicate 51, 94, 243
indicated 89, 128, 273
indicators 172, 220
indirect 172, 195, 208, 260
indirectly 3
individual 23, 210-211, 249, 251, 258, 276
industry 1-2, 75, 101, 180, 211
influence 26, 39, 105, 140, 150-151, 210, 241-242, 254
influenced 264
influences 255
inform 86, 114-115, 126
informal 258
informed 208
infosec 88
ingrained 92
inherently 113
inhibit 80
in-house 2
initiated 165, 197, 239
Initiating 4, 146
initiative 11, 141
injury 264
Innovate 69
innovative 197, 234
inputs 31, 36, 55-56, 96, 136, 147, 149, 157
inside 26, 140
insider 131

insight 34, 64, 127
insights 1-2, 9, 62
inspector 127
install 134
installed 134
instances 109
instead 2, 207
Institute 168
instructed 159
insurance 264
integrate 77
integrated 131, 147, 200, 227
integrity 24, 239
intended 3, 74, 137, 256
intense 80
INTENT 18, 29, 43, 54, 69, 85, 100
intention 3
intentions 244
intents 153
interest 136, 203, 214, 235
interested 276
interests 24, 231
interim 253
internal 1, 3, 31, 103, 111, 138, 172, 174, 213, 229
internally 61
interpret 11
intervals 158, 174, 229
interview 1, 276
introduce 115, 123
introduced 102, 104, 117, 133, 138, 250, 257
inventory 171
invest 26, 78
investing 2
investment 21, 112, 202, 222
involve 89, 124, 132
involved 19, 60, 122, 157, 171, 187, 201, 208, 210, 215, 231, 234, 236, 265, 274, 276
involves 159
involving 265
issues 18-21, 23-26, 48, 75, 77, 157, 161-162, 165, 183-184, 211, 229, 248, 254, 256
iteration 158
itself 3, 22, 115

justified278
keeping 54, 134
keyboard 123
knowing 51
knowledge 1-2, 10, 31, 59, 86, 88-90, 93, 106, 127, 172, 210, 231-232, 245, 249, 275
labeled 208
language 135
larger 21
largest 188
latest 9
laundry 160
leader 37, 219, 221
leaders30, 36, 93, 201-202, 255
leadership 35, 71, 151
leakage 52
learned 1, 7, 88, 205, 268, 276, 278
learning 88, 241, 244, 253
leaving106
legacy 124
lesson 276
lessons 7, 79, 88, 205, 268, 278
letter 162
Leveling 178
levels 24, 37, 73, 94, 169, 171, 201, 205
leverage 30, 88, 189, 198
leveraged 31, 117
levers 133
liability 3
license 137
licensed 3, 137
lifecycle 58, 80
Lifetime 10, 106
likelihood 153, 216, 220
likely 71, 74, 151, 199, 219-222, 241
limited 10
limiting 116
linked 35, 141, 161
listed 194, 225
listen 248-249
little 2, 160
loaded227
location 106, 151, 241

locked 64
logical 136, 182, 184
longer 1, 56-57
long-term 95
looked 1
losses 25
lowest 124, 182, 260
lurking 125
machines 19, 49, 64-65, 104-105, 107, 114, 131, 134, 137, 142
maintain 76, 85, 136, 202
maintained 171, 175, 208, 259
majority 94
makers 270
making 205-206, 210, 278
malicious 124, 136
malware 46
manage 69, 101, 104, 114, 131, 137, 139-140, 163-165, 174, 180, 191, 196, 205, 214-215, 230, 254, 279
manageable 39, 225
managed 8, 51, 66, 221, 226, 269
management 4-6, 9-10, 19, 21-22, 25, 29-30, 39, 44-45, 55, 57, 59-60, 72, 80, 82, 87, 93, 101, 105, 111, 114-115, 119, 121, 126, 128, 131, 133-135, 138, 141-142, 153, 155-157, 159, 165-167, 174, 178, 187-188, 193, 199, 201, 205, 207, 211-213, 215-217, 220, 222, 225-227, 229, 231-232, 235-236, 244, 249, 256-257, 262, 268, 270, 273, 275
manager 8, 10, 18, 32, 36, 76, 160, 211, 221, 229, 235, 279
managers 4, 145, 171, 187, 222, 233
manages 155, 266
managing 4, 124, 145, 150, 159, 244
mandatory 239, 277
manipulate 117
manner 25, 117, 171, 195, 211, 251
manual 202
mapped 37, 94
marked 166
market 180, 188, 215, 263
marketable 215
marketer 8
marketing 162, 167, 181
material 149, 171-172, 181, 203, 228, 260
materials 3, 165, 248

matrices 96, 163
Matrix 4-6, 151, 163, 207-208, 221
matter 31, 48, 251
matters 241
mature 49, 56, 105
maturity 132
maximise 264
maximizing 188
meaning 178, 248
meaningful 250
measurable 34, 39, 234, 258
measure 4, 10, 19, 30, 40, 43, 46, 49, 51, 69, 148, 151, 197-198, 203, 253
measured 45, 96, 202, 250
measures 44-49, 51, 94, 201, 217, 234, 237, 252
measuring 243
mechanical 3
mechanism 276
mechanisms 44, 94, 97, 142
median 106
medium 251, 262
meeting 38, 93, 165, 199, 210-211, 236, 244, 247-249, 276
meetings 32-33, 39, 160, 174, 242, 248, 270
member 6, 35, 38, 235, 248, 252, 254
members 1, 29, 32-33, 38, 143, 154, 157, 192, 210, 213, 215, 246-253, 258, 272, 279
membership 253, 258
memorable 250
memory 237
mental 264
mergers 125
message 231-232
messages 128, 213, 249
metadata 59
method 129, 136, 155, 179, 189, 196, 204, 250
methods 36, 155, 167, 171, 198, 201, 219, 230, 249, 265
metrics 5, 46, 90, 157, 159-160, 174, 203-204
Microsoft 188
migrate 140
migrating 123
milestone 5, 148, 180, 182, 226
milestones 39, 150, 172, 182
million 112

minimize 90, 172, 220, 256, 271
minimum 70, 72, 133, 266
minority 24
minutes 38, 211, 247
missing 101, 143, 178-179, 279
mission 209
mistakes 278
mitigate 25, 76, 271
mitigated 2, 270
mitigating 113
mitigation 155, 191, 229
mobile 252
mobilized 154
models 122, 264
modern 212
modified 71
modify 110, 131
module 117
moments 63
Monday 1
monetary 19
monitor 74, 86, 97, 158, 197, 273
monitored 91, 157, 176, 190, 212
monitoring 6, 85-86, 89, 95, 97, 159, 175, 184, 256, 261, 264, 272-273
monolithic 123, 140
months 1
Morale 151
morning 1
mostly 37
motivated 211
motivation 151
motive 205
multiple 50, 76, 104, 226, 230, 260, 264
mutual 153
narrative 167, 180
narrow 65
national 152, 154
nature 117, 142
nearest 12
necessary 61, 78, 96, 197, 225, 227, 234, 239, 246, 258
needed 2, 24, 26, 31, 56, 76, 89, 94, 196-197, 213, 225, 254, 270, 276

negative 191
negatively 233
negotiated 92, 272
neither 3
network 5, 22, 33, 36, 44, 54, 81, 86, 101, 111, 113, 119-120, 123, 127-128, 131, 137-138, 140, 182
networking 127
networks 108, 116, 128, 132
Neutral 11, 18, 29, 43, 54, 69, 85, 100
normal 73, 92
normalize 136
Notice 3
noticing 242
notified 220, 231, 274
notify 248
notion 143
number 26, 40, 52, 67, 83, 98, 135, 144, 185, 215, 280
numbers 249
numerous 116, 126, 274
objection 20, 23
objective 8, 108, 148, 151, 154, 172, 200
objectives 2, 21, 23, 25, 29, 35, 153, 192, 199, 212, 223, 236, 254, 258
observable 77
observed 71
observing 168
obstacles 20, 197
obtain 103, 120, 268
obtained 34, 225
obvious 251
obviously 11
occurred 142
occurrence 50, 220, 237
occurring 81
occurs 19, 86, 146, 221
office 108-109, 146, 212, 235, 265, 274
officer 1, 227
officers 228
officials 274
offshore 161
one-time 8
ongoing 49, 87, 96, 176, 190
on-going 158

online 90
operate 24, 237
operating 6, 63, 92, 111, 116, 131, 199, 248
operation 73, 91, 189, 243
operations 10, 21, 32, 44, 47, 87, 90, 92, 132, 142, 149, 199
operators 90
opponent 241
opponents 254
optimal 71, 73, 79, 266
optimize 73, 79
options 18
ordered 1
organized 178
orient 93
oriented 194
origin 162
others 138, 160, 191, 197, 199, 207-208, 210, 213, 215, 221, 225, 258, 264
otherwise 3, 80, 200
outcome 11, 186, 247
outcomes 78, 197, 244, 263, 276
outgoing 137
outlier 178
outlook 187
outpace 104
output 30, 50, 94
outputs 36, 96, 184
outside 78, 146, 270
outsource 148, 187
outsourced 187
outweigh 47
overall 10-11, 23, 48, 75, 79, 147, 167, 182, 256, 267
overcome 197
overflow 141
overhead 171, 208, 260-261, 278
overload 102
overlook 213
overlooked 211, 270
overly 128
oversight 65, 212
overtime 179
owners 169
ownership 82, 86, 153

package 172-173
packages 171-172, 260
parameters 91, 104
paramount 222
Pareto 60, 175
parking 211
partial 57
particular 49, 51, 107, 138
parties 2, 126, 243, 274
partner143
partners 19, 154, 276
password 37, 62, 110, 126, 139
passwords 121
patched 65
patches 59, 104, 115, 118, 128, 135-136, 142-143
patching 47, 118
pattern 178
patterns 24
payment 273-274
payments 230
pedigree 104
pending 239
people8, 21, 106, 109, 119, 138, 146, 188, 203, 207-208, 215, 221, 232-233, 235, 245, 263-264, 271
percentage 19, 73, 75, 77, 79, 163
perform 32, 38, 40, 73, 78, 92, 114, 117, 134, 160, 185, 219, 268
performed 57, 69, 82, 95, 110, 117, 119, 163, 176-177, 217, 227, 253, 261
performing 102, 130, 132
perhaps 263
perimeter 80
period 171, 195, 261
periodic 230
permission 3
person 3, 195, 207
personal 55, 134, 278-279
personally 24, 163
personnel 19, 174, 182, 243
pertaining 35
pertinent 132
phases 79, 213, 216, 270
phishing 112

physical 128, 140
placed 56, 243
placements 244
planned 48-49, 146, 176, 188, 194, 208, 217, 230, 276-277
planning 4, 9, 86, 92-93, 96-97, 153, 155, 157, 165, 172, 177, 184-185, 235
platform 252
platforms 95, 252
playing 2
pocket 190
pockets 190
points 26, 40, 48, 52, 67, 83, 98, 144, 205
policies 63, 90, 96-97, 105, 107, 120, 140, 209, 264
policy 23, 25, 33, 47, 65, 81, 125, 133, 140, 149, 152, 167, 184, 212, 273, 278
political 80, 180, 219, 221, 254
population 101, 142
portfolio 233
portion 2
portray 60
position 210, 265
positioned 197-198
positive 102, 156, 231
possess 258
possible 62, 65, 70, 80, 85, 118, 131, 193, 226, 234, 258, 264
potential 21, 70, 81, 162, 187, 214, 217, 223, 257
practical 69, 85, 235
practice 152
practiced 147
practices 10, 24, 37, 72, 79, 88, 90, 97, 125, 129, 140-141, 153, 155, 157, 212, 268
practicing 106
praise 251
precaution 3
precede 182
predict 60
prediction 178
predictor 185
preference 133
preferred 276
pre-filled 9
Premium 215

prepare 187, 210, 225, 228
prepared 1, 142, 147
present 49, 63, 94, 253
presented 1, 246
preserve 40
prevent 22, 26, 167, 174
prevented 273
previous 31, 180, 192, 203, 266
previously 217, 239
priced 172
primary 185
principles 97, 153, 212
priorities 47, 49-50
prioritize 44, 47-49, 51-52
Priority 48, 178
privacy 120, 131
private 76-77, 154
privileges 108
probably 185
problem 18, 21, 29, 31, 34, 39, 59, 235, 241, 262
problems 20-23, 50, 81, 89, 161-162, 165, 203, 257, 278
procedure 64
procedures 10, 61, 63, 90, 92-93, 97, 113, 120, 134, 171-172, 174, 184, 195, 201, 203, 228, 230, 248-249, 272-273
proceed 219
process 4-6, 8, 10, 20, 30-31, 34, 36-37, 43-47, 49-51, 54-66, 71, 73-74, 81, 86-89, 92-95, 146-148, 153-154, 158-161, 163, 165-168, 172, 175, 184, 187, 189, 205-206, 215, 219, 228-229, 233-234, 241, 246, 251, 256, 262-264, 266, 268, 270, 272, 279
processed 57
processes 1, 37, 49, 55-56, 60, 63, 65, 90, 147, 152-154, 167, 212, 215, 229, 233, 238, 240, 243, 249, 256, 268
processing 56
procuring 172
produce 1, 147, 154, 184, 236, 246
produced 278
produces 179
producing 163
product 3, 63, 80, 97, 105, 108, 113, 126-127, 139, 151, 158, 160, 167, 180, 199-201, 203, 215, 222, 224, 235-236, 239, 247, 254, 262-265, 278
production 73, 77, 88, 130, 147, 167, 249
productive 134

products 3, 58, 64, 72, 76, 135, 137, 153, 163, 193, 236, 240
profile 82, 139, 218
program 19, 30, 32, 87, 92, 96, 101-102, 105, 107-109, 112, 116, 119-121, 125-127, 129, 131, 154, 210, 234, 256
programme 134, 234
programmer 71, 115
programs 154, 235, 238
progress 29, 148, 197, 205-206, 253, 278
prohibit 273
project 4-9, 32, 37-38, 40, 44, 50, 71-74, 76, 79-80, 85, 92-93, 95-96, 103, 105, 107, 116, 119, 122-123, 125, 128-129, 131, 136, 143, 145-155, 157-160, 162-163, 165, 168-169, 174-176, 178, 180-182, 185-195, 197, 199-200, 207, 209-213, 215-222, 225-227, 229, 233-235, 239, 246-247, 254, 256-259, 262, 266, 268-271, 274, 276, 278-279
projected 171-172
projects 4, 20, 39, 57, 60, 69-71, 80, 90, 96, 105, 123, 143, 145-146, 149, 163, 165, 187-188, 192, 195, 200, 220, 222, 230, 233, 236, 262-264, 270
promotion 210
promptly 256
proofing 71
proper 101, 110, 143
properly 36, 135, 141, 161, 279
properties 104
proponents 254
proposal 180, 227
proposals 227-228
proposed 78, 155, 211, 217, 231, 266
protect 37, 66, 75, 81, 120
protected 64, 105, 128, 141
protecting 64
protection 94, 215
protocols 61, 102, 140
proved 268
provide 19, 70, 73-74, 79, 102, 122, 150, 172, 188, 195-197, 212, 258
provided 2, 12, 86, 97, 108, 112, 132, 227, 265, 278
provider 30, 61-62, 92, 114
providers 226
provides 185, 244
providing 150, 165, 180, 243-244
provision 108, 137, 211, 225

public 76-77, 136, 154
publicly 128
published 273
publisher 3
purchase 9, 272
purchased 171
purchasing 1-2
purpose 4, 10, 86-87, 89, 92-93, 109, 139, 185, 191, 197, 205, 250-252, 258
pursuing 2
putting 104
qualified 32
quality 5-6, 10, 51, 57, 66, 76, 89, 157, 174-175, 194, 201, 203-205, 209, 212, 225, 243-244, 256, 273, 279
quantity 228
quarterly 137
question 11, 18, 29, 43, 54, 69, 85, 100, 153
questions 8-9, 11, 254, 278
quicker 65
quickly 10, 57, 221
raised 165, 211
rather 261
rating 136, 227
ratings 75, 82, 129, 227-228
rationale 241, 260
readiness 123, 175
readings 97
reality 102, 220
realize 2
realizing 1
really 8, 81, 100, 105, 159
reason 217
reasonable 155-156, 158, 174, 193, 226
reasonably 172
reasons 32, 56
reassess 211, 225
re-assign 179
reassigned 200
recasts 195
receipt 171
receipted 264
receive 9-10, 32, 48, 231, 247
received 29, 243, 250

recently 92, 122
recipient 24, 274
recognize 4, 18-24, 26, 251
recognized 20-21, 23-26, 211, 214, 245, 250, 254, 272
recognizes 18
recommend 165-166
record 55, 103
recorded 201, 237, 264
recording 3, 202, 248-249, 272
records 171, 208, 274
recovery 61, 91
recurrence 223
re-design 61
reduce 44, 48, 73, 81, 154
reduced 131
reducing 93, 133
reduction 81, 133
reference 136
references 280
reflect 59, 168
refreshed 2
refreshing 96
refuses 223
regard 154
regarding 55, 140, 195, 227, 235, 279
Register 4-5, 150, 160, 213, 217, 264
registries 77
regular 20, 29, 39, 55, 165-166, 193, 266
regularly 24, 33, 39, 116, 120, 134, 188, 199, 270
regulation 37, 139
regulatory 35, 37, 114
reject 159
relate 76, 240
related 24, 72, 79, 93, 105, 122, 134, 165, 171, 201, 213, 237, 262
relation 152, 244
relations 217
relative 136, 250
release 69, 104, 109, 131, 158, 167, 193, 203, 213, 225
releases 58, 129, 266
relevance 45
relevant 24, 39, 96, 129, 136, 199, 231
reliable 38, 55
reliably 107

relied 24
relieved 2
remaining 191, 198, 277
remediate 22, 57, 78, 82, 91, 121, 133, 140
remediated 50, 73, 77, 79
remedies 48
remember 189
remote86
remotely 21
remove 62, 71, 77
removed 91, 124
repair 193, 226
rephrased 10
replanning 171
report 6, 47-48, 60, 97, 113, 202, 235, 243, 247, 258, 266
reported 50, 138, 165, 244, 254, 262
reporting 59, 63, 73, 79, 89, 96, 120, 135-136, 202, 207, 215, 260-261
reports 2, 30, 150, 156, 193, 207, 278
repository 174, 193, 225
represent 65, 118, 239
reproduce 133
reproduced 3
reputation 102
request 6, 20, 96, 140, 160, 200, 237, 239
requested 3, 239
requests 221, 237, 272
require 33, 36-37, 40, 62, 184, 220
required 30, 32-33, 36-38, 46, 58, 64, 75, 82, 146-147, 159, 161, 168, 176-177, 186, 189, 232, 248, 276
requires 146, 228
requiring 116, 138, 150, 274
research 166, 249
Reserve 195
reserved 3
reside 142, 174, 193
residual 71, 171
resilience 44, 87
resilient232
resolution 165
resolve 25, 179, 246
resolved 203, 211, 256

resource 5, 118, 153, 158, 172, 175, 178-179, 184-185, 187-188, 193, 211, 226, 235
resources 2, 4, 9, 38-39, 71-72, 95, 112, 138, 146, 154, 177-178, 182, 186, 190, 195, 198-200, 229-231, 252, 254, 258, 261
respect 3
respected 272
respond 18, 108, 131, 153
responded 12
response 19, 21, 86, 89, 91, 93-95, 101, 103, 128, 267
responses 218, 244
responsive 190, 197
restricted 55, 62
result 66, 75-76, 81, 88, 172, 197, 199, 232, 239, 274
resulted 85
resulting 65, 156
results 9, 21-22, 38-39, 50, 69-72, 75, 77, 80-81, 86, 90, 97, 153-154, 178, 188, 198, 202, 234, 243, 269, 273
Retain 100
return 202
returned 55
reveal 128
revert 73
review 10, 34, 49-50, 56, 66, 70, 72, 74-75, 82, 88, 96, 103, 123, 182, 192, 194-195, 199, 225, 243, 249, 253, 272
reviewed 19, 37, 88, 127, 158, 229
reviewer 127
reviewers 250
reviewing 128
reviews20, 75, 119, 165, 182, 193, 215, 229
revised 63, 85
revisions 274
revisit 242
Reward 235
rewarded 24
rewards 81, 90
rights 3, 26, 55, 76, 136, 141
robustness 180
rollback 127
rolled 141
rotation 101
routed 119
routine 88
routinely 57, 109, 244

running 101, 111, 131
safeguards 95
safely 224
safety 155, 248, 265
sample 227
sampling 175
sanctions 135
satisfied 268-269
satisfies 262
satisfy 76
savings 30, 63
scandal 265
scanned 103, 116
scanner 117, 134
scanning 22, 73, 113, 117, 128, 132, 134
scenario 93
scenes 2
schedule 5, 30, 72, 153, 174, 182, 191-192, 194, 200, 217-218, 225, 230, 239, 246, 266, 277, 279
scheduled 193, 226, 270
schedules 173, 183
scheduling 157, 211
schema 96
scheme 95, 140
schemes 126
Science 189
scientific 189
Scorecard 4, 12-14, 233
scorecards 90
scores 14, 130
scoring 10, 119
screening 155
scripting 81
scripts 101, 114
second 12
secret 2, 124
secrets 1, 120
section 12, 26, 40, 52, 67, 83, 98, 144
sections 97, 167
sector 263
secure 20, 33, 49-50, 57, 70, 72, 79, 101, 103, 106, 111-112, 123, 125, 131, 133, 138-139
securely 100, 126

securing 124
security 19-22, 24, 31, 34, 36, 39-40, 44-45, 47-48, 50-51, 56-58, 60-61, 64, 70-73, 76, 79-82, 85-87, 89, 92, 94-95, 97, 101-105, 107, 109-112, 114-115, 118, 120-134, 136, 138-140, 142-143, 150, 167, 239, 276
seeing 81
segment 119
segmented 32
segments 37, 260
selected 71, 74, 76, 110, 197-198, 220, 253
selecting 155
selection 6, 57, 227, 250
self-help 2
sellers 3
sending 109, 132
senior 201-202
sensitive 51, 56, 58, 61, 64-66, 102, 120, 130
sequence 176, 182
sequencing 157, 188
series 11
seriously 72
server 107, 112, 135
servers 114
Service 1-4, 8, 51, 58, 92, 126, 180, 199, 201, 235-236, 243, 278
services 3, 21, 46, 58, 78, 94, 107, 127, 187-188, 196, 217, 233, 243-244, 260, 266, 268, 272, 274
serving 243
session 125, 141, 177
setting 260
settings 139
severely 61
severity 65, 106, 109, 217
shared 89, 100, 107, 109, 139, 198, 242
sharing 114, 120, 139, 260
shopping 1
shortest 234
short-term 251
should 8, 18-19, 26, 30-31, 40, 45-46, 48, 51, 55, 63, 71-73, 76, 78, 81, 93, 100, 102-103, 107-108, 113, 118, 121, 139, 146, 148, 150, 154-155, 176-177, 185, 187, 190, 195, 200, 208-210, 217-218, 220-221, 223, 227-229, 231, 233, 240, 246-247, 256-257, 271, 278
signatures 184
signers 274

signing 57
similar 31, 38, 60, 73, 176, 178, 203, 207, 255
simple 258, 263, 272
Simply 9
simulation 132
single 50, 73, 78, 261
single-use 8
situation 2, 22, 43, 217, 262
skilled 33
skills 33, 106, 123, 133, 146, 207, 215, 231, 233, 245, 250, 270, 279
smaller 104, 154
smooth 278
soccer 1
social 244
software 24, 33-34, 40, 47, 54, 56-57, 61-62, 74-75, 79-80, 85, 94-95, 97, 102, 104, 107, 109, 111-112, 115, 122, 124-125, 133, 135, 137, 140-141, 147, 157, 167-168, 216, 222, 231, 266
solely 112
solicit 36, 248
solution 1, 50, 69-74, 77-80, 82, 85-86, 223, 256, 266
solutions 65, 70, 73, 75-76, 78, 80-81, 217
Someone 8
something 135, 139, 141, 155, 199, 207
source 6, 24, 72, 107, 109, 111, 118, 125-126, 131, 227, 229, 243
sources 54, 60, 77
special 59, 97, 228
specific 9, 22, 34, 36, 39, 63, 92, 116, 122, 167, 176, 180-181, 184-185, 199, 209, 219, 227, 235, 240, 253
specified 95, 108, 207, 260-261
specify 39-40, 73, 101, 171
spending 2, 111, 119
sphere 26, 39
sponsor 21, 156, 268
sponsored 37
sponsors 19, 246, 270
stability 50
staffed 39
staffing 90, 94, 156, 194
staffs 252
stages 155, 211, 225
standard 8, 92, 94, 147, 184, 261, 266

standards 10-11, 88-92, 94, 96-97, 167-168, 201-202, 240, 260
started 9, 125
starting 10
stated 162, 171, 201, 203, 272
statement 4, 11, 148, 158, 165, 195, 200
statements 12, 26, 39-40, 52, 59, 67, 83, 98, 144, 159
statistics 165
status 6, 106, 109, 111, 123, 128, 152, 158-159, 165, 174-175, 229, 235, 247, 260, 262, 266
steering 158, 211, 229
storage 64, 237
stored 55, 57, 104, 107
Strategic 212, 244
strategies 153, 191, 229, 241-242
strategy 23, 87, 116, 213, 228, 231, 272
strength 152
strengths 268
strive 233
strong 31, 210
strongest 133
Strongly 11, 18, 29, 43, 54, 69, 85, 100, 237
Structure 5, 72, 114-115, 169, 185, 232
structured 225
structures 258, 260
subdivided 172
subject 9-10, 31, 132
submitted 239
sub-teams 258
subtotals 196
succeed 250
success 19, 22, 40, 130, 147-148, 151, 175, 182, 225, 236, 242, 251, 256, 270
successful 1, 82, 91, 124, 153-154, 185-186, 195, 213, 234, 236, 276
successor 174
suddenly 219
suffered 250
sufficient 154, 237, 272
suggest 237
suggested 89, 239
suggesting 104
suitable 44, 171, 222, 265

suitably 243
summary 51
sunbelt 127
Sunday 1
superior 1
supervisor 130, 210, 252-253, 278
supplied 76, 109
supplier 115, 193, 229, 273
suppliers 36, 47, 75, 272
supplies 193, 268
supply 180
support 3, 8, 34, 48, 78, 91, 94, 132, 135, 139, 143, 147, 173, 184, 209, 211, 222, 232, 242, 267
supported 35, 66, 102, 278
supporting 93, 97, 201, 205
supportive 209, 212
supports 25
supposed 207
surface 89, 110, 121
survival 64
SUSTAIN 4, 100
sustaining 95
symptom 18
system 10, 21, 57, 82, 93, 106, 111, 115-117, 119-120, 123, 125, 134-135, 140, 142, 161, 167-168, 172, 185, 237, 239, 242-244, 262-263
systems 1, 20, 22, 43, 47, 59, 65, 90, 103, 105, 108, 110, 116-117, 126, 128, 131-132, 152, 174, 188, 230, 243, 262, 269, 272
tackling 65
tactics 241-242
tailor 82, 88
tailored 2
taking 236, 261
talking 8
target 35, 231-232
targeted 109
targeting 138
targets 129, 148, 234, 262
tasked 87
teaming 248
technical 75, 80, 94, 123, 140, 147, 194, 227-228, 256
technique 187, 233
techniques 46, 86, 89, 108, 114, 124, 137

technology 1, 81, 104, 113, 124, 146, 161, 180, 188, 243, 248-249
template 192
templates 8-9
test-cycle 205
tested 72, 80, 95, 108
tester 141
testing 39, 69-71, 81, 92, 103, 106, 108, 121, 123-124, 130, 133, 139, 141, 167, 203, 265
themes250
themselves 1
therefore 138, 223
theyre 160
things 101, 146, 204, 207, 219, 257
thinking 56, 78, 121
thorough 240
thoroughly 165
thought 127, 248, 255
threaded 62
threat 26, 50, 52, 71, 117, 131-132, 143
threaten 192
threats 1-2, 63, 71, 94, 104, 116, 118, 122, 129, 136, 224
throttling 116
through 20, 50, 57, 110, 165, 241
throughout 3, 132, 182, 188
throughput 188
Thursday 1
time-bound 39
timeframe 178, 197
timeline 167, 239
timely 25, 38, 105, 117, 142, 171, 195, 211, 278
timeout 125
timetable 182
Timing 213, 246
together 47, 100, 207, 248
tolerate 216
tolerated 177
toolkit 1-2
toolkits 1-2
topology 113
toward93, 236
towards 2, 129
traces 128

tracked 110, 126, 165, 226
tracking 31, 159, 201, 211
trade-in 272
trademark 3
trademarks 3
tradeoff 228
trained 33, 35-36, 114, 168, 202, 215
training 90, 93, 97, 167, 210, 232, 236, 249, 252, 272
Transfer 12, 26, 41, 52, 67, 83, 86, 90, 98, 144, 266
transition 159
translated 34
treated 130
trending 201
trends 60, 156, 165, 201
trigger 19
triggers 199, 229
trouble 97
trusted 111, 119, 137
trying 8, 120, 148, 158, 204, 223, 243
turnaround 178
unable 25
unaware 1
uncovered 2, 161
underlying 70
understand 34, 79, 81-82, 160, 187, 248, 250, 264
understood 57, 161, 221
undertaken 93, 103, 272
unified 70, 73, 78
unique 2, 195, 200
uniquely 254
Unless 8
unpatched 75, 106
unplanned 249
unprepared 1
unpriced 171
unresolved 184
untimely 135
unused 134
update 1, 25, 59-60, 112, 132, 191, 199, 277
updated 9-10, 59, 158, 166, 174, 182, 193, 212, 226, 230
updates 10, 19, 49, 90, 100, 104, 107-108, 115, 117, 119-120, 122, 126, 129, 133-134, 136, 140-142, 266
updating 61-62, 96, 158

upfront 231
upgrades 59
urgent 237
useful 78, 89, 170, 215, 278
usefully 10
usually 1
utility 190
utilize 57, 63, 92, 97
utilized 58-59
utilizing 1, 74
validate 263
validated 31, 34, 37, 60, 96, 157
validation 40, 253, 263
validity 256
valuable 8, 125, 129
values 202
variables 50, 94, 242, 253
Variance 6, 188, 250, 260
variances 194, 260-261
variation 18, 38, 43-44, 49, 51, 54, 60, 93
variations 161
various 211, 225
vendor 21, 33-34, 78, 109-110, 127, 131, 146, 193, 273
vendors 38, 65, 108, 113, 174, 273
verbally 207
verified 10, 31, 34, 37, 60, 104, 180
verifier 140
verify 94, 166, 191, 199, 238, 262, 275
version 266, 280
versions 30-31, 106, 138
vetted 131
vetting 167
viable 169
vice-versa 276
vigorously 258
violate 167
violations 167
virtual 118, 249, 252
visible 128
vision 156, 209
visions 154
visitors 102
visits 193

visualize 189
voices 150
volatility 215, 265
volume 208
vulnerable 66, 93, 112, 116
waited 2
walking 2
warnings 124
warranty 3
weaknesses 33, 110, 115, 117, 131, 134, 168, 268
weeknights 1
whether 8, 276
wholesaler 193
willing 70, 200, 215
window 178
winning 121
wishes 245
wishing 64
within 1-2, 26, 46, 81, 102, 110, 119, 128, 136, 143, 176, 190, 235, 239, 248, 253, 269, 273
without 1, 3, 12, 139, 161, 219, 240, 274
workaround 80
workdays 217
worked 72, 129, 155, 207, 221, 255, 270, 279
worker 130
workers 188
workflow 241
workflows 38
workforce 123, 211
working 2, 37, 74, 118, 125, 167, 191, 207, 241, 264
Worksheet 5, 189, 197
worksheets 227
writing 163, 201, 207
written 3, 110
youhave 177, 191
yourself 127, 210