

Sample Patch & Vulnerability Readiness Responses

This sample response file demonstrates how an SME might complete the **Vulnerability Management Questionnaire** and the **Patch Management Readiness Checklist**.

It provides realistic scoring and can be used to test the readiness scoring engine.

☐ Scoring Format

Each question is scored as:

- 0 = Not implemented
 - 1 = Partially implemented
 - 2 = Mostly implemented
 - 3 = Fully implemented
-

☐ Sample Responses (CSV Style View)

question_id,score

1,2

2,2

3,1

4,2

5,3

6,1

7,2

8,3

9,2

10,1

11,2

12,1

13,1

14,2

15,2

16,1

17,1

18,2

19,2

20,3

21,2

22,1

23,1

24,3

25,2

26,2

27,1

28,2

29,1

30,1

31,1

32,2

33,2

34,2

35,1

36,2

37,2

38,1

39,2

40,1

41,1

42,2

43,2
44,1
45,2
46,2
47,1
48,2
49,1
50,1
51,0
52,1
53,1
54,2

☐ Interpretation

These sample responses reflect a **moderately mature** vulnerability & patch management posture.

Strengths

- Patch cycles exist and run consistently
- Inventory management mostly reliable
- Cloud workloads partially monitored
- Reasonable patch compliance rates

Weaknesses

- Limited testing before deployment
- Weak emergency patching capability
- Weak tracking of repeated failures
- Lack of full vulnerability triage
- Minimal threat intelligence usage

Expected Score Range

A submission like this will score approximately **80–95**, which fits the “**Moderate Readiness**” maturity level.

☐ How to Use This File

You can use this sample to:

- Test the scoring engine

- Populate dashboards
- Provide examples during audits
- Train staff on how to complete the questionnaire
- Demonstrate toolkit usage in documentation

Place it under:

```
data/sample_responses.md
```
