Tech Policy Primer

Bug Bounty Program Readiness Score Guide

SUPPORTING INFORMATION FOR THE AGENCY READINESS SCORECARD

Ahmed Amer, Di Cooke, Rob Lever, Julia Pan

This is a mock guide to enable federal agencies to develop their own bug bounty programs (BBPs). This guide should accompany a fully implemented BBP Readiness Survey to assess whether an agency is adequately prepared to execute a bug bounty program (BBP) on their agency systems. (See this demo video for a sample of how the BBP Readiness Survey would look, and Appendix B for the flow of the survey.) The survey would produce a Readiness Scorecard for the agency. This guide assists agencies in interpreting the Readiness Scorecard results.

INTRODUCTION TO THE BUG BOUNTY PROGRAM

Summary

The Readiness Scorecard and this accompanying Guide are tools for agencies to gauge their levels of preparedness to execute bug bounty programs (BBPs). Specifically,

- The Readiness Scorecard helps agencies gauge how ready they are to conduct a BBP according to a series of 6 predetermined criteria that have been customized specifically for federal agencies.
- The Readiness Survey (a demo of which can be seen here) can be used to obtain your agency's Readiness Scorecard and find out what your readiness scores are for each of the 6 Readiness Factors.

- This document, the Guide, provides further information on the 6 Readiness Factors, their scoring thresholds, and guidelines for how to improve your score.

What Are Bug Bounty Programs and Their Benefits?

Please see the BBP 101 Informational Document for information on BBPs, as well as to learn more about the advantages of executing a BBP and some successful programs conducted by federal agencies in recent years.

Preparing Your Agency System(s) for Bug Bounty Programs

To make effective use of a BBP, government agencies must be ready for such an exercise, and the Readiness Scorecard offers a means of assessing such readiness. The 6 criteria evaluated for the Readiness Scorecard are:

1. Budget;
2. Staffing;
3. The Vulnerability Disclosure Policy;
4. Vulnerability Management;
5. Security Assessments; and
6. Backlog Management.

In an ideal world, all agency computing systems would be protected against every known vulnerability at all times. In reality, maintaining good cyber hygiene and improving security postures is an ongoing task that needs to be completed against an ever evolving security landscape. Agencies should establish good vulnerability discovery, reporting requirements, and remediation policies, and, and compliance with Cybersecurity and Infrastructure Security Agency (CISA) directives will help agencies effectively embrace such policies.

When it comes to evaluating the security of systems, it helps to have a diverse group of experts seeking out bugs and vulnerabilities that might not be detected otherwise. BBPs offer an efficient and cost-effective means of improving systems' security by allowing for scrutiny by a broader array of cybersecurity experts than any typical agency could bring to bear on its own infrastructure.

However, without adequate readiness, the benefits of a BBP would not be realized. For example, if an agency conducts a BBP without first identifying currently known vulnerabilities, it could end up paying unnecessary bounties. In order to prepare agencies, the BBP Readiness Scorecard evaluates agency readiness on 6 criteria that target particular traits and requirements of government agencies and their systems. This document explains each of the 6 criteria in greater detail and describes what would constitute high, low, or medium scores for each criterion. It also provides guidance on how to improve low or medium scores.

The guidance provided in this document and the criteria of the Readiness Scorecard are tailored to the needs of government agencies. Federal agencies both benefit from existing CISA support and guidance and face different challenges in readiness than would be encountered by a typical private sector organization. For example, budget and staffing limitations, particularly for agencies with less developed cybersecurity operations, may not be easy to overcome without assistance and coordination from CISA. A scorecard should be assessed by each agency that is considering participation in a BBP, but since only specific systems would be elected for participation in a BBP, criteria should be evaluated on a per-system basis.

The intended audience of the agency readiness scorecard BBPs is the Chief Information Office (CIO) or the Chief Information Security Officer (CISO) and their office.

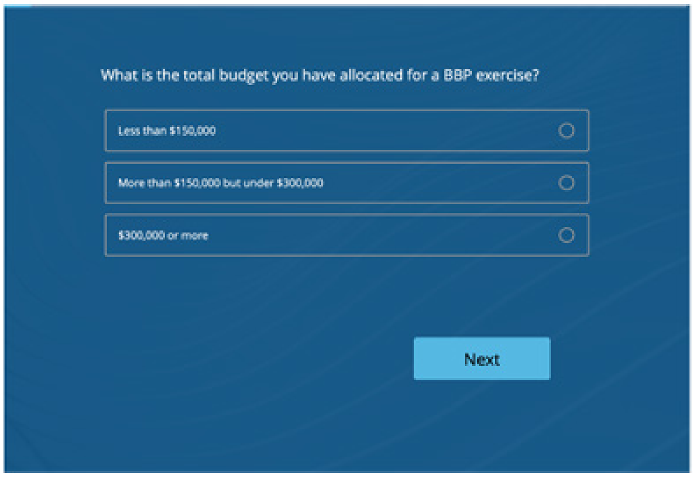
Using the Readiness Survey, Scorecard, and Guide

Below is the step-by-step guide to using the BBP Readiness Survey, Scorecard, and Guide.

Step One: Take the Readiness Survey (a demo of which can be found here, and the flow of which can be found in the appendices).

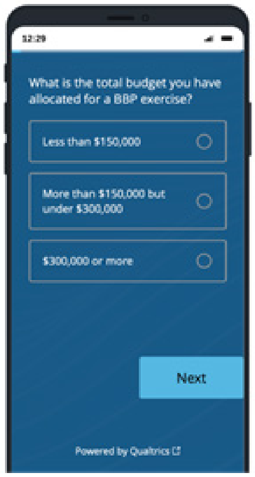
You will be asked a series of questions pertaining to each of the Readiness Factors. If you require more information about a question, you can go to the relevant Readiness Factor in this document.

Survey questions adapt to answers as you progress. A sample survey question for one Readiness Factor is shown below; flowcharts for all 6 Readiness Factors are included in the Appendix.



What is the total budget you have allocated for a BBP exercise?

- Less than $150,000 ○
- More than $150,000 but under $300,000 ○
- $300,000 or more ○



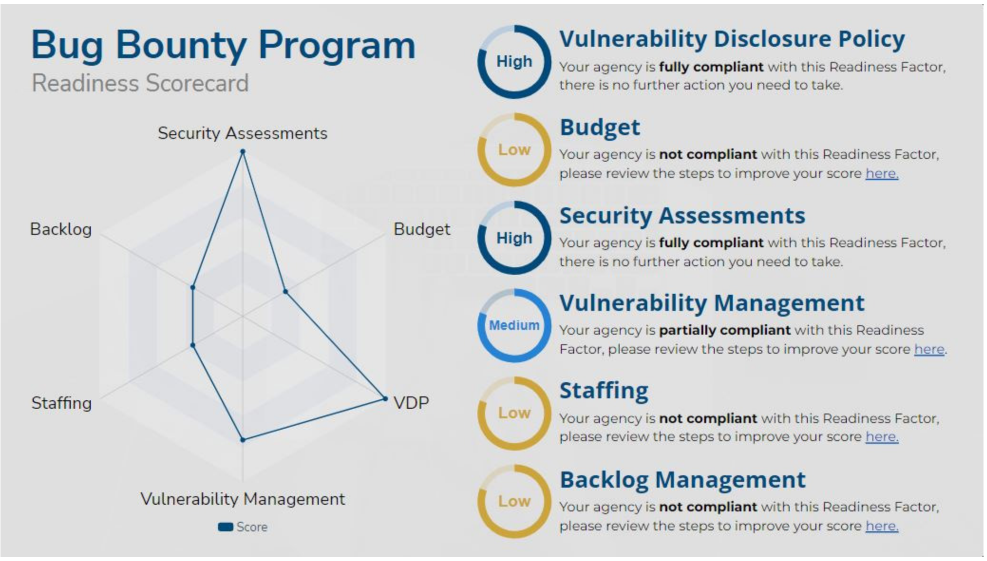
What is the total budget you have allocated for a BBP exercise?

- Less than $150,000 ○
- More than $150,000 but under $300,000 ○
- $300,000 or more ○

Step Two: Once you have completed the Readiness Survey, your Readiness Scorecard will be generated. An example scorecard is shown below.

The Readiness Scorecard gives you scores for each of the 6 Readiness Factors, along with links to additional information about your score and how to improve it. You can also navigate directly to this information by going to the relevant Readiness Factor in this document.

Step Three: Take the necessary steps to improve your score as per the rest of this document’s



Bug Bounty Program
Readiness Scorecard

High — **Vulnerability Disclosure Policy**
Your agency is **fully compliant** with this Readiness Factor, there is no further action you need to take.

Low — **Budget**
Your agency is **not compliant** with this Readiness Factor, please review the steps to improve your score here.

High — **Security Assessments**
Your agency is **fully compliant** with this Readiness Factor, there is no further action you need to take.

Medium — **Vulnerability Management**
Your agency is **partially compliant** with this Readiness Factor, please review the steps to improve your score here.

Low — **Staffing**
Your agency is **not compliant** with this Readiness Factor, please review the steps to improve your score here.

Low — **Backlog Management**
Your agency is **not compliant** with this Readiness Factor, please review the steps to improve your score here.

suggestions, and update CISA on your actions.

READINESS FACTORS

This section shares more details on:

- Each individual Readiness Factor;
- Information necessary to determine the level of readiness;
- What constitutes "high," "low," and "medium" for each factor; and
- Steps to improve a low or medium Readiness Factor score.

The 6 Readiness Factors are:

1. Budget;
2. Staffing;
3. The Vulnerability Disclosure Policy;
4. Vulnerability Management;
5. Security Assessments; and
6. Backlog Management.

I. Budget

To ensure that your agency is able to afford the cost of running a BBP, you must identify the typical range of costs. This section breaks down the costs associated with running a BBP for you to compare against your agency's budget. It also provides concrete thresholds for whether you have scored low, medium, or high in this Readiness Factor, and provides next steps for improving your agency's score.

The Costs of Running a BBP

Total Cost

Based on vendor fees and financial payouts, the estimated total cost to run a BBP is $300,000–$500,000, depending on the program's systems scope and the coverage of vendor services. More detailed information on the cost breakdown can be found in Appendix A.

Core Costs

1. **Hiring a vendor:** $150,000–$450,000
2. **Providing payouts to researchers:** $50,000–$150,000

Possible Additional Costs

1. **Hiring internal staff to support BBPs:** This is dependent on agency requirements and headcount costs. You will need to speak to the relevant contact in your agency for this information.
2. **Transaction fees:** This is dependent on the agency's costs of money transfer and acquisition fees. You will need to speak to the relevant contact in your agency for this information.

Budget Readiness Levels

Low Readiness (Not Ready)

Your agency does not have an adequate budget to dedicate to the vendor fees for a BBP. This means your agency budget for a BBP is **less than** $150,000–$450,000.

Medium Readiness (Partially Ready)

Your agency is able to cover the costs of vendor fees, but unable to pay additional costs. This means your agency budget for a BBP is **more than** $150,000–$450,000, but your agency budget either **cannot cover** the entire required payout ($50,000–$150,000) or **cannot pay** for one of the following two potential costs:

- The additional staff you might need to support the internal services necessary to run a BBP (dependent on agency); or

- The associated government transaction fees (dependent on agency).

High Readiness (Fully Ready)

You have the budget required to pay for both internal services and vendor services. This means there is enough budget to cover **all of the below:**

- $300,000–$500,000 for vendor fees and required payouts;
- If necessary, additional staff required to support a BBP; and
- Any associated government transaction fees.

How can you improve your readiness score from low to medium or high?

Your options to increase funding for a BBP include the below.

Obtaining funding through inclusion in your agency's future budget. This might include:

- Speaking to internal contacts to discuss whether a program's existing budget can be allocated to BBP fees; and/or
- Reaching out to CISA to obtain support for including a BBP in the future budget.

Submitting funding to Congress. This might include working with the program office that will be responsible for submitting the BBP fees request to Congress.

Speaking with CISA about additional funding options. Potential funds might include:

- The Technology Modernization Fund (TMF), a fund to help agencies "better secure sensitive systems and data, and use taxpayer dollars more efficiently."
    - You can read about the details of the fund on the TMF website and review their contact guidelines here. Make sure to notify CISA if you decide to submit a TMF funding request, as they may be able to support your bid.
- The American Rescue Plan (ARP), a fund to "support investments that move the government

to a consistent baseline of maturity in cybersecurity and privacy protections."

- You can read about the details of the fund on the ARP website and review their contact guidelines here. Make sure to notify CISA if you decide to submit an ARP funding request, as they may be able to support your bid.

How can you improve your readiness score from medium to high?

Your options to increase your funding for a BBP include the below

- **Reviewing the options from "How to improve scoring from low to medium or high" in this document.** If you have scored medium, we suggest that you prioritize first speaking with CISA and exploring additional funding options, as those may be easier to accomplish than revising your agency's budget.
- **Reviewing the anticipated scope of your proposed BBP.** Narrowing the types of vulnerabilities your BBP covers may reduce vendor costs and restrict the overall amount required for payout. Any vulnerabilities that researchers discover that are outside the defined scope will not result in a payout and should be managed via your agency's Vulnerability Disclosure Policy.
- **Developing and running an internal BBP pilot as a "proof of concept" to encourage funding support for a later, full BBP program.** For example, you can partner with another agency you already have strong relations with, and have their system's owner(s) target certain types of predefined vulnerabilities. Examples of specific vulnerabilities could include the OWASP Top Ten Web Application Security Risks. You can also request CISA's support with such a BBP "proof of concept."

II. Staffing

Agencies will need to determine whether they have adequate staffing to implement a BBP; they will also need to address the deployment of their personnel. Both technical staff and administrative staff will be needed to manage the program, and personnel will be needed to interact with any vendors or platforms.

Technical roles include:

- Those who identify and evaluate candidate systems and liaise with system owners;
- System administrators and evaluators;
- Vulnerability, forensic, and security analysts;
- Threat and risk assessment managers; and
- Information, security, and privacy officers.

Administrative roles include:

- Authorization and oversight officers;
- Business and mission owners and program managers;
- Acquisition, financial, and operations officers; and
- Other support staff, including designated reporting and liaison roles.

Agencies without management and IT staff who can be dedicated to a BBP exercise will not be prepared to implement the BBP and may need to redeploy personnel from other areas or arrange for temporary reassignments to ensure sufficient support.

Staff already deployed for vulnerability disclosure programs may be assigned responsibilities for bug bounties. New tasks for administering budgets and contracting and managing bug bounty payments may require additional staff, training, or deployment from other organizational units. Agencies may also get technical assistance and guidance from CISA and/or the US Digital Service or the Defense Digital Service.

Staffing Readiness Levels

Low Readiness (Not Ready)

You are at a low level of readiness if you do not have designated staff with knowledge of BBPs; you are unable to effectively liaise with vendors executing a BBP and system owners; or you do not have designated staff to address contracting and budgeting needs for a BBP.

Medium Readiness (Partially Ready)

You are at a medium level of readiness if you have designated staff with knowledge of what a BBP exercise would entail, but who are not prepared to:

- Address the technical execution of a BBP by effectively liaising with a BBP provider;
- Implement and manage a BBP within the agency; or
- Address administrative execution of a BBP by providing support for budgeting and/or contracting and reporting.

High Readiness (Fully Ready)

You are at a high level of readiness if you have designated staff with knowledge of BBPs who are prepared to address both the technical execution and the administrative execution of a BBP. This means:

- Having designated staff to effectively liaise with a BBP provider (or being able implement and manage a BBP yourself); and
- Having designated staff to perform budgeting, contracting and payment, and reporting for a BBP.

How can you improve your readiness score from low to medium?

To improve readiness from low to medium, a program will need to be able to execute one of the following tasks:

- **Designate staffing for technical execution of a BBP**. This could be achieved by:
  - Educating and training existing staff (whether dedicated cybersecurity staff or system owners) regarding bug bounties; or
  - Recruiting new cybersecurity or system management staff (via temporary cross-agency assignments, or by hiring for a dedicated position) with BBP knowledge.
- **Arrange for budgeting and contracting support for a BBP exercise.** This could be achieved by:

- Assigning staff within existing in-agency programs;
- Reassigning staff within or between agencies through temporary assignments or the pursuit of joint programs; or
- Recruiting additional staff.

How can you improve your readiness score from medium to high?

If your agency lacks the staffing needed either to execute a BBP or to administratively plan and support a BBP, then you should consult with CISA about the adequacy of designated staffing levels. You can also address deficiencies by:

- Educating and training existing staff (whether dedicated cybersecurity staff or system owners) on bug bounties;
- Recruiting new cybersecurity or system management staff (via temporary cross-agency assignments or by hiring for a dedicated position) with BBP knowledge;
- Reassigning staff within existing in-agency programs;
- Reassigning staff within or between agencies through temporary assignments or the pursuit of joint programs; or
- Recruiting additional staff.

III. Vulnerability Disclosure Policy

A Vulnerability Disclosure Policy (VDP) is a "formal policy that describes the activities that can be undertaken in order to find and report vulnerabilities in a legally authorized manner. Such policies enable federal agencies to remediate vulnerabilities before they can be exploited by an adversary — to immense public benefit." CISA's Binding Operational Directive (BOD) 20-01 requires all government agencies (excluding national security systems and certain systems operated by the Department of Defense or the intelligence community) to publish VDPs. To evaluate whether your agency is compliant with BOD 20-01, please review the below options and identify the level of VDP readiness that most accurately represents your agency.

VDP Readiness Levels

Low Readiness (Not Ready)

You are not compliant with BOD 20-01. This means:

- Your system is not defined as a national security system, nor is it a prespecified system operated by the Department of Defense or the Intelligence Community that is excluded from the BOD 20-01.
    - If you are unsure whether your system falls under this category and is thereby exempt from BOD 20-01, please speak with the relevant agency contact or email CISA.
- Your agency has not taken steps to execute a VDP for your agency's system as per BOD 20-01.

Noncompliance with the VDP requirements means that at least four of the below criteria apply:

- You have not enabled receipt of unsolicited vulnerability reports.
- You have not developed and published a VDP.
- You are unable to adhere to your vulnerability disclosure handling procedures.
- Your agency system scope schedule is behind CISA's required deadlines.
- You are not fully compliant with CISA's vulnerability reporting requirements.

Medium Readiness (Partially Ready)

You are partially compliant with BOD 20-01. This means:

- Your system is not defined as a national security system, nor is it a prespecified system operated by the Department of Defense or the Intelligence Community that is excluded from the BOD 20-01.
    - Note: If you are unsure whether your system falls under this category and is thereby exempt from BOD 20-01, please speak with the relevant agency contact or email CISA.
- Your agency has taken some steps to execute a VDP for your agency's system as per BOD 20-

01.

Partial compliance with the VDP requirements means that at least two of the following criteria apply:

- You have not enabled receipt of unsolicited vulnerability reports.
- You have not developed and published a VDP.
- You are unable to adhere to your vulnerability disclosure handling procedures.
- Your agency system scope schedule is behind CISA's required deadlines.
- You are not fully compliant with CISA's vulnerability reporting requirements.

High Readiness (Fully Ready)

You are fully compliant with BOD 20-01. This means:

- Your system is defined as a national security system or as a prespecified system operated by the Department of Defense or the Intelligence Community that is excluded from the BOD 20-01.
  - Note: If you are unsure whether your system falls under this category and is thereby exempt from BOD 20-01, please speak with the relevant agency contact or email CISA.
- Your agency has taken steps to execute a VDP for your agency's system as per BOD 20-01.

Full compliance with the VDP requirements means that all of the below criteria apply:

- You have enabled receipt of unsolicited vulnerability reports.
- You have developed and published a VDP.
- You are adhering to your vulnerability disclosure handling procedures.
- Your agency system scope schedule aligns with CISA's required deadlines.
- You are fully compliant with CISA's vulnerability reporting requirements.

How can you improve your readiness score from low to medium or high?

Read the BOD 20-01 and identify which parts you are noncompliant with, then execute BOD 20-01 using CISA's implementation guidelines. More details on the key steps of the implementation guidance can be found here. CISA also provides helpful resources for identifying noncompliance with BOD 20-01 programs.

If you have difficulty understanding how to become compliant, then you should read the BOD 20-01's FAQ for additional support or contact CISA for further direction. You should also ask yourself the following questions to identify the cause of noncompliance:

- Is it a continuing issue with understanding what is required?
- Is it a technical issue?
- Is it a financial issue?
- Is it a bandwidth issue?

How can you improve your score from medium to high?

Read the BOD 20-01 and identify which parts you are noncompliant with, then execute BOD 20-01 using CISA's implementation guidelines. More details on the key steps of the implementation guidance can be found here. CISA also provides helpful resources for identifying noncompliance with BOD 20-01 programs.

If you have difficulty understanding how to become compliant, then you should read the BOD 20-01's FAQ for additional support, or contact CISA for further direction. You should also ask yourself the following questions to identify the cause of noncompliance:

- Is it a continuing issue with understanding what is required?
- Is it a technical issue?
- Is it a financial issue?
- Is it a bandwidth issue?

Iv. Vulnerability Management

How your agency identifies and responds to software vulnerabilities is an important part of assessing your readiness to run a BBP. If your agency does not have a process to remediate reported vulnerabilities, then a BBP is too mature for your agency. For direction, you can refer to some of CISA's Binding Operative Directives (BODs), which help define federal standards for vulnerability remediation — specifically compliance with sections in BOD 19-02 (Vulnerability Remediation Requirements for Internet-Accessible Systems) and BOD 20-01 (Develop and Publish a Vulnerability Disclosure Policy). (You can find more about how to develop handling procedures under the VDP template section of BOD 20-01.)

If a vulnerability were discovered in your system, does your organization have a system in place to receive reports and respond?

Vulnerability Management Readiness Levels

Low Readiness (Not Ready)

Your agency has not developed, documented, or implemented handling procedures of vulnerabilities or remediation plans for critical and high vulnerabilities. This means your agency **does not have a process to address more than two** of the dimensions below.

From BOD 19-02 Review and Remediate Critical and High Vulnerabilities:

- Remediation of critical vulnerabilities within 15 calendar days of initial notification;
- Remediation of high vulnerabilities within 30 calendar days of initial notification; and
- A remediation plan if agencies aren't able to resolve within the specified timeframe.

From BOD 20-01 Vulnerability Disclosure Handling Procedures:

- Tracking reports;
- Internal coordination with those who need to know about the vulnerabilities;
- Process for triage, prioritization, and resolution development;
- Handling reports out of scope;
- Management of communications with a vulnerability reporter;

- Evaluation of the potential previously unknown impact of reported vulnerabilities; and
- Procedures around federal incident reporting.

Medium Readiness (Partially Ready)

Your agency has developed, documented, and implemented some handling procedures of vulnerabilities or remediation plans for critical and high vulnerabilities. This means your agency **has a process to address at least five** of the following dimensions:

- Remediation of critical vulnerabilities within 15 calendar days of initial notification;
- Remediation of high vulnerabilities within 30 calendar days of initial notification;
- A remediation plan if agencies aren't able to resolve within the specified timeframe;
- Tracking reports;
- Internal coordination with those who need to know about the vulnerabilities;
- Process for triage, prioritization, and resolution development;
- Handling reports out of scope;
- Management of communications with a vulnerability reporter;
- Evaluation of potential previously unknown impact of reported vulnerabilities; and
- Procedures around federal incident reporting.

High Readiness (Fully Ready)

Your agency has developed, documented, and implemented handling procedures of vulnerabilities as well as remediation plans for critical and high vulnerabilities. This means your agency **has a process to address all** of the dimensions below:

- Remediation of critical vulnerabilities within 15 calendar days of initial notification;
- Remediation of high vulnerabilities within 30 calendar days of initial notification;
- A remediation plan if agencies aren't able to resolve within the specified timeframe;

- Tracking reports;
- Internal coordination with those who need to know about the vulnerabilities;
- Process for triage, prioritization, and resolution development;
- Handling reports out of scope;
- Management of communications with a vulnerability reporter;
- Evaluation of potential previously unknown impact of reported vulnerabilities; and
- Procedures around federal incident reporting.

How can you improve your score from low to medium or high?

- **Use GSA's Public Disclosure of Vulnerabilities Handbook** for guidance on how to craft your agency's handling procedures.
- **Designate a technical point person** at your agency who can communicate with CISA about cyber hygiene scanning access (ncats@hq.dhs.gov) and remediation plans (fnr.bod@hq.dhs.gov).

How can you improve your score from medium to high?

- **Consider publishing your vulnerability handling procedure** so your team can easily find and refer to the policy. This will also instill confidence with vulnerability reporters that your agency takes the process seriously.
- **Train, hire, or outsource staff** to address critical and high vulnerabilities as notified by CISA.

V. Security Assessment Maturity

Federal agencies should have an internal security assessment process before running a BBP. If your internal team hasn't already tested your agency's systems, BBPs can become an expensive way to identify vulnerabilities. One way to measure your agency's security assessment maturity is through compliance with the Federal Information Security Modernization Act (FISMA). Your Inspector General (IG) submits an annual evaluation report of your agency's progress on FISMA compliance.

The Office of Management and Budget (OMB) and CISA released FY 2022 CIO (Chief Information Officer) FISMA Metrics that provide metrics "towards the implementation of the Administration's priorities and best practices that strengthen Federal Cybersecurity." The current administration seeks to replace "point-in-time assessments with ongoing and continuous risk assessments that will allow agencies to prioritize cybersecurity risks with accurate, real-time information about the agency's posture and threats." The administration is also interested in prioritizing proactive testing tools such as penetration testing, VDPs, red team exercises, bug bounty programs, and more.

Security Assessment Maturity Readiness Levels

Low Readiness (Not Ready)

Your agency has not achieved an effective information security program. FISMA effectiveness is determined by agency IGs, who have the discretion to consider agency-specific factors such as mission, cyber challenges, and resources. A noncompliant FISMA agency **does not have** any of the following resources in place:

- An information system inventory;
- risk categorization;
- A system security plan;
- Security controls (defined by NIST-800-53);
- A three-tiered risk assessment using the NIST Risk Management Framework (NIST-800-39); or
- Certification and accreditation through yearly reviews.

Medium Readiness (Partially Ready)

According to your IG, your agency has achieved a partially effective information security program. A semi-compliant FISMA agency **has some of the below:**

- An information system inventory;

- Risk categorization;
- A system security plan;
- Security controls (defined by NIST-800-53);
- A three-tiered risk assessment using the NIST Risk Management Framework (NIST-800-39); or
- Certification and accreditation through yearly reviews.

High Readiness (Fully ready)

According to your IG, your agency has achieved an effective information security program. A compliant FISMA agency has **all of the below:**

- An information system inventory;
- Risk categorization;
- A system security plan;
- Security controls (defined by NIST-800-53);
- A three-tiered risk assessment using the NIST Risk Management Framework (NIST-800-39); and
- Certification and accreditation through yearly reviews.

How can you improve your scoring from low to medium or high?

- **Request help** from the United States Digital Service, Defense Digital Service, your agency's digital service team, or CISA to get up to speed on FISMA best practices, vulnerability inventories, and security assessments.
- **Find resources** from CISA's list of free cybersecurity services and tools to get started on maturing your security assessment processes.
- **Utilize resources** from CISA's Cyber Resource Hub and Cyber Hygiene Services, which offer professional security assessments to agencies at no cost. For BBP readiness, the vulnerability

scanning, risk and vulnerability assessment, and web application scanning resources are especially helpful.

How can you improve your scoring from medium to high?

- **Work with your IG.** They can assist you with implementing recommendations from their annual report.
- **Email CISA to request a Remote Penetration Test for your agency.** Penetration tests are BBPs with a more focused scope.

VI. Backlog Management

To understand if an agency is ready for a BBP, it is first important to know how effectively and efficiently the agency is handling the remediation of its current vulnerabilities. Effective agencies are those that are already at a good level of security and have addressed known exploited vulnerabilities. Efficient agencies address their vulnerabilities in a timely manner.

Even if agencies bring all their systems into full compliance with the relevant CISA directives that detail vulnerability disclosure and remediation policies (BOD 20-01, BOD 19-02, and BOD 22-01), there can still be varied levels of backlog management as the system owners work to address known vulnerabilities within the required time windows. Backlog management, therefore, is both an estimate of system readiness for participation in BBP and a measure of the maturity and efficiency of the vulnerability management for a particular system. Agencies that score high on backlog management should have confidence in a timeline for vulnerability remediation. Agencies that have a plan for reaching such a state are at a medium level of readiness.

An agency that has received a positive scorecard report on its cyber hygiene posture (provided by CISA to its agency leadership) should already have a remediation plan for known vulnerabilities. Agencies that are not fully compliant with directive BOD 22-01 and lack an ongoing vulnerability remediation policy will have a lower backlog management score, as being in a high state of readiness requires a knowledge of timelines for remediation.

Backlog Management Readiness Levels

Low Readiness (Not Ready)

You are not compliant with either BOD 20-01 or BOD 22-01, and you are unable to offer definite timelines for remediation of known exploited vulnerabilities.

Medium Readiness (Partially Ready)

You are partially compliant with BOD 20-01 and BOD 22-01, or you have a known timeline for compliance but lack a clear timeline for remediating known exploited vulnerabilities.

High Readiness (Fully Ready)

You are partially compliant with BOD 20-01 and BOD 22-01 or have a known timeline for compliance, and you have a clear timeline for remediating known exploited vulnerabilities.

How can you improve your readiness score from low to medium or high?

For each system under agency control, **identify a point of contact to drive work toward compliance with BOD 20-01.** This person would also be responsible for establishing a timeline for such compliance.

If you are unable to develop a plan for compliance with the available guidance, reach out to CISA for additional support.

How can you improve your readiness score from medium to high?

To achieve a high level of readiness, you must be able to **estimate a timeline for remediation and measure average vulnerability remediation rates for your system.** This implies either:

1. Compliance with BOD 22-01; or
2. Partial compliance to the point of being able to estimate a timeline for remediating known exploitable vulnerabilities.

Once you have planned a timeline for such compliance, it is also necessary to estimate the remediation time required for ongoing compliance. This is more than simply citing the required remediation windows; it also requires confidence in evaluating the true expected remediation rates for your system. To achieve this, employ and evaluate a continuing remediation policy. If you are unable to develop a plan for continued compliance with the available guidance, reach out to CISA for additional support.

Appendix A: Agency Readiness

See below for background information on how the estimated fees for BBPs were calculated.

Overall Cost

In the past, government agencies have paid between $300,000–$500,000 in total for BBPs, as seen at USASpending.gov.

Core Costs

Core costs of implementing BBPs include:

1. **Hiring a vendor.** Vendors who run BBPs typically cost around $150,000–$450,000 to hire. This number is dependent on:

   a. The extent of vendor services provided, as some are more inclusive than others; and

   b. The size and complexity of the system(s) the BBP is being run on.

   To get a quote for running a BBP on your system(s), you can either reach out to a vendor to speak with them directly (examples of well-known vendors include Bug Bounty | Bugcrowd, HackerOne Bug Bounty Platform for Businesses, and Scale Beyond Bug Bounty with Crowdsourced Security | Synack) or reach out to CISA to obtain information on the vendor costs of past BBPs.

2. **Providing payouts to researchers.** Your agency will be responsible for payouts to researchers who have found vulnerabilities within the scope of the BBP's coverage. Past agencies' payouts have been between $50,000–$150,000 for each BBP.

   To get an idea of how much you are likely to pay, you should speak with your potential vendor or reach out to CISA to obtain information on the payout costs of past BBPs.

Possible Additional Costs

Possible additional costs of implementing BBPs include:

1. **Hiring internal staff to support BBPs.** Depending on the inclusivity of the services of the vendor that you choose, you might need to hire temporary or permanent staff to deal with program coordination or remediation efforts. If this is necessary, you will need to speak with contacts inside your agency to discuss the costs of additional personnel in the needed roles. Depending on the amount of support, CISA may also be able to provide some financial assistance. (However, there may be no need for additional personnel.)

2. **Transaction fees.** Hiring external vendors to run a BBP on your system(s) may lead to additional fees. You should speak with your internal procurement and acquisitions teams to understand what these fees might be. You should also reach out to CISA to obtain information on possible transaction fees associated with deploying BBPs.

Appendix B: Readiness Survey Logic

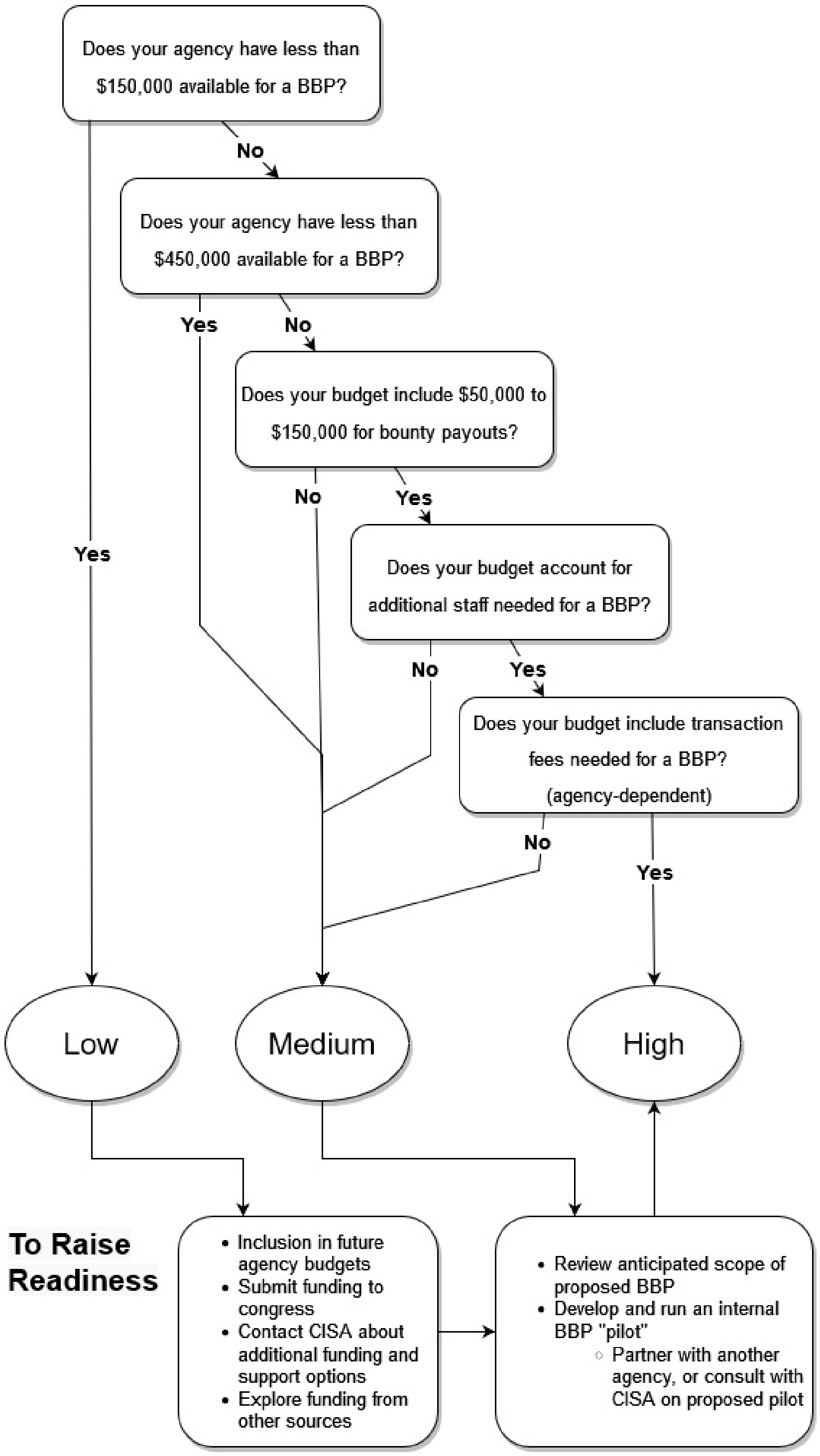
The full set of flowcharts for each of the readiness indicators in the BBP Readiness Survey are included below. Each flowchart provides a high-level sketch of the progression of questions, and subsequent recommended actions, of the initial draft of the BBP Readiness Survey.

Our video demo was implemented as a simple Qualtrics survey, with questions presented or withheld using that particular platform's "display logic" rules. Recommended actions and results were also presented using those roles and so would be generated for each user before the conclusion of the survey. An added benefit of this approach is that the same survey can be completed by multiple individuals within an agency, allowing for the collection of aggregated readiness data across multiple systems within an agency. However, this kind of functionality (and the necessary customization or gate questions needed to narrow the scope of the survey to the expertise or focus of an individual respondent) was not included in this demo. Such a use would be best tailored to individual agencies that might prefer a distributed internal evaluation mechanism.

These flowcharts are provided to allow for the straightforward mapping of the survey logic to any preferred implementation platform. The flowcharts provided cover all 6 readiness factors, using an individual flowchart for each factor:

1. Budget;
2. Staffing;
3. The Vulnerability Disclosure Policy;
4. Vulnerability Management;
5. Security Assessments; and
6. Backlog Management.

Budget Readiness



Does your agency have less than $150,000 available for a BBP?

Does your agency have less than $450,000 available for a BBP?

Does your budget include $50,000 to $150,000 for bounty payouts?

Does your budget account for additional staff needed for a BBP?

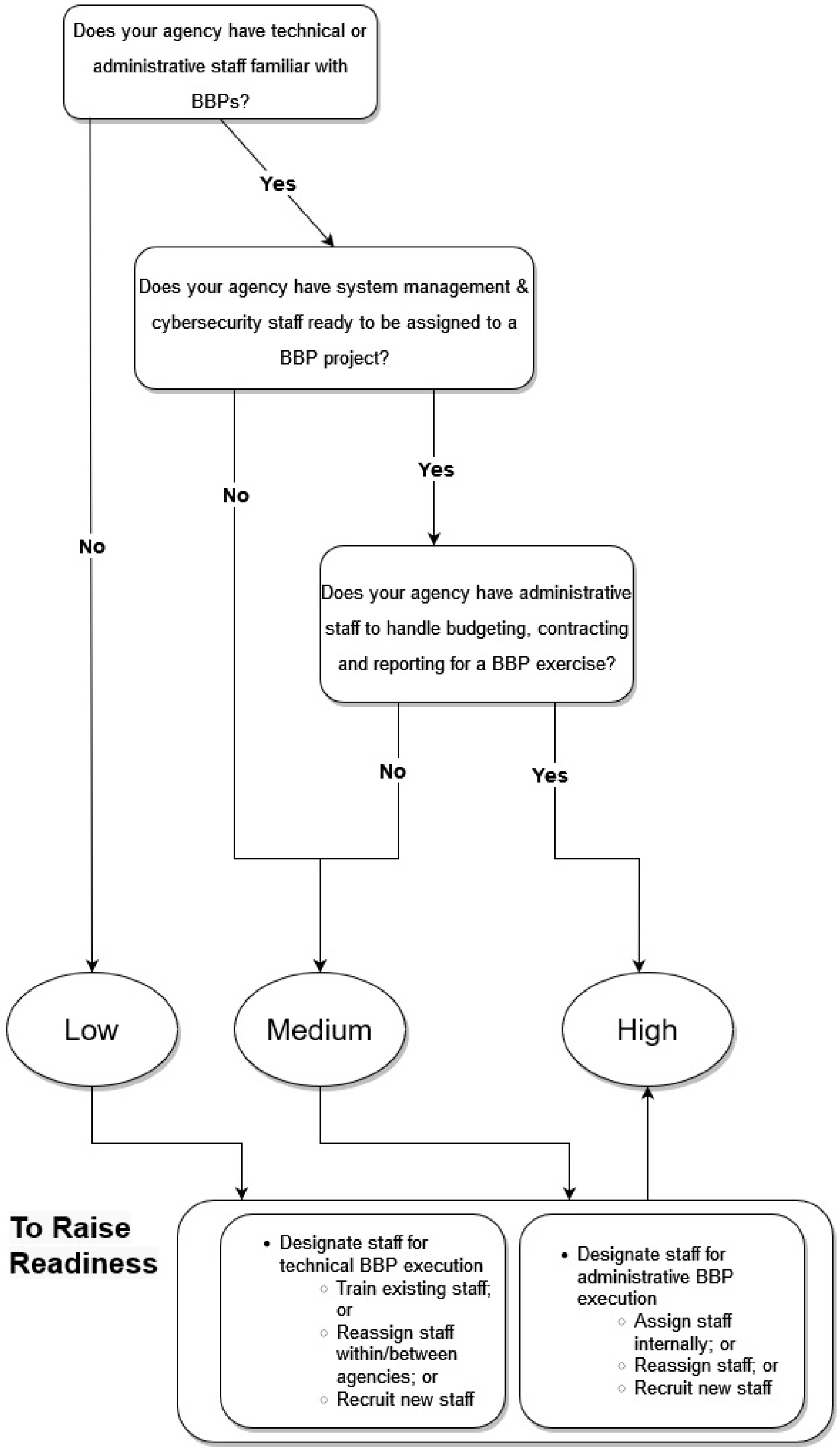
Does your budget include transaction fees needed for a BBP? (agency-dependent)

To Raise Readiness

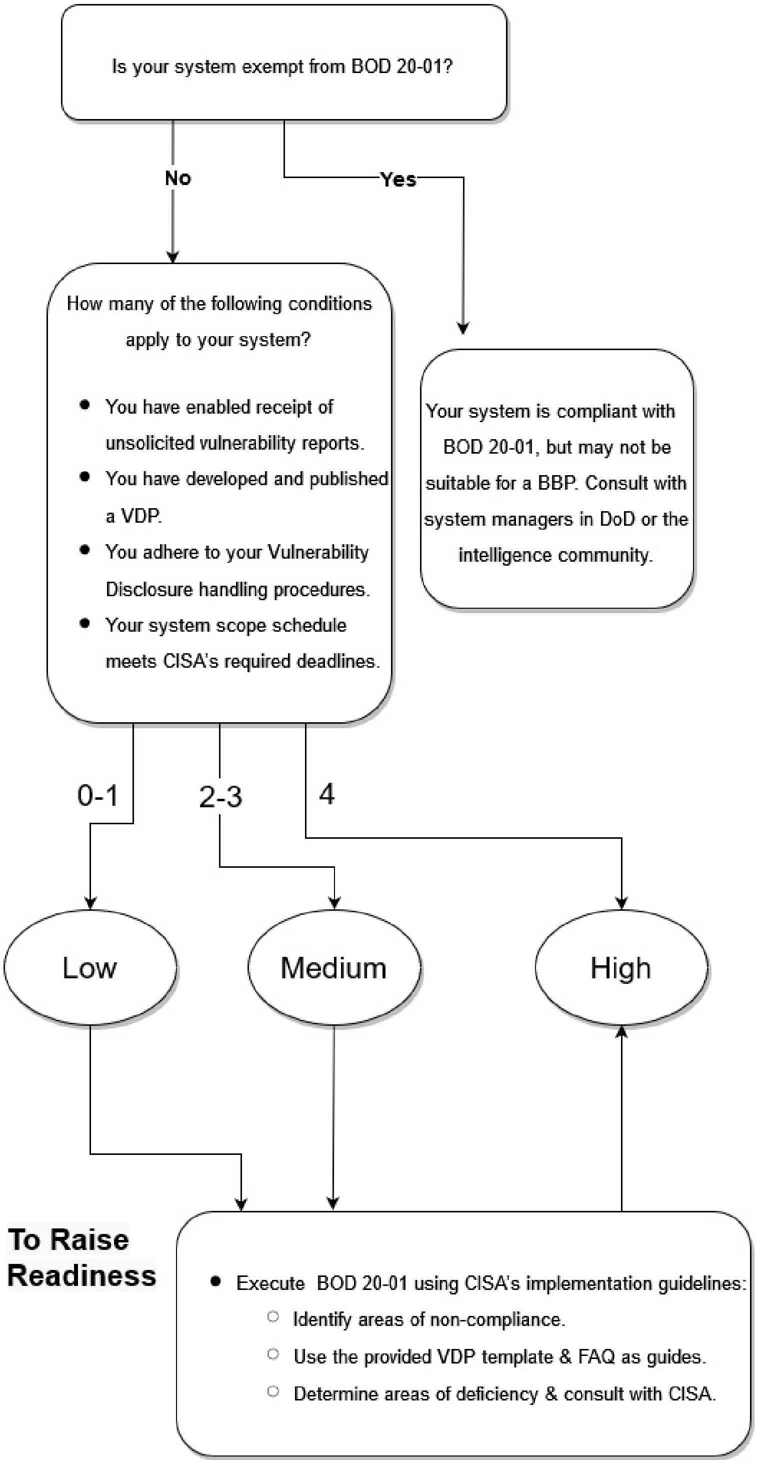
- Inclusion in future agency budgets
- Submit funding to congress
- Contact CISA about additional funding and support options
- Explore funding from other sources

- Review anticipated scope of proposed BBP
- Develop and run an internal BBP "pilot"
    - Partner with another agency, or consult with CISA on proposed pilot

Staff Readiness


Does your agency have technical or administrative staff familiar with BBPs?
Yes
No
Does your agency have system management & cybersecurity staff ready to be assigned to a BBP project?
No
Yes
Does your agency have administrative staff to handle budgeting, contracting and reporting for a BBP exercise?
No
Yes
Low
Medium
High
To Raise Readiness
• Designate staff for technical BBP execution
◦ Train existing staff; or
◦ Reassign staff within/between agencies; or
◦ Recruit new staff
• Designate staff for administrative BBP execution
◦ Assign staff internally; or
◦ Reassign staff; or
◦ Recruit new staff

VDP Readiness



Is your system exempt from BOD 20-01?

How many of the following conditions apply to your system?

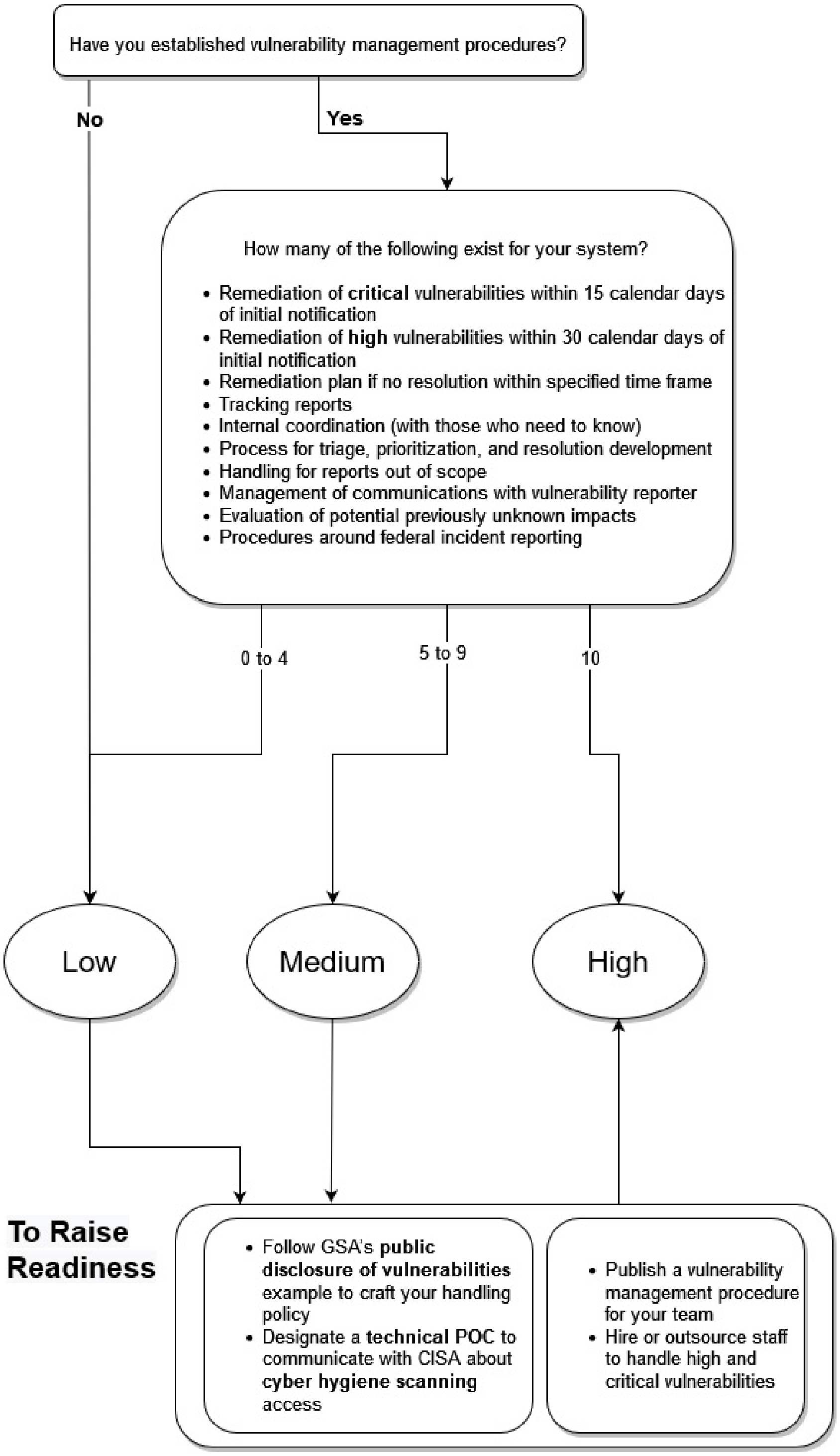
- You have enabled receipt of unsolicited vulnerability reports.
- You have developed and published a VDP.
- You adhere to your Vulnerability Disclosure handling procedures.
- Your system scope schedule meets CISA's required deadlines.

Your system is compliant with BOD 20-01, but may not be suitable for a BBP. Consult with system managers in DoD or the intelligence community.

To Raise Readiness

- Execute BOD 20-01 using CISA's implementation guidelines:
  - Identify areas of non-compliance.
  - Use the provided VDP template & FAQ as guides.
  - Determine areas of deficiency & consult with CISA.

Vulnerability Management Readiness



Have you established vulnerability management procedures?

How many of the following exist for your system?

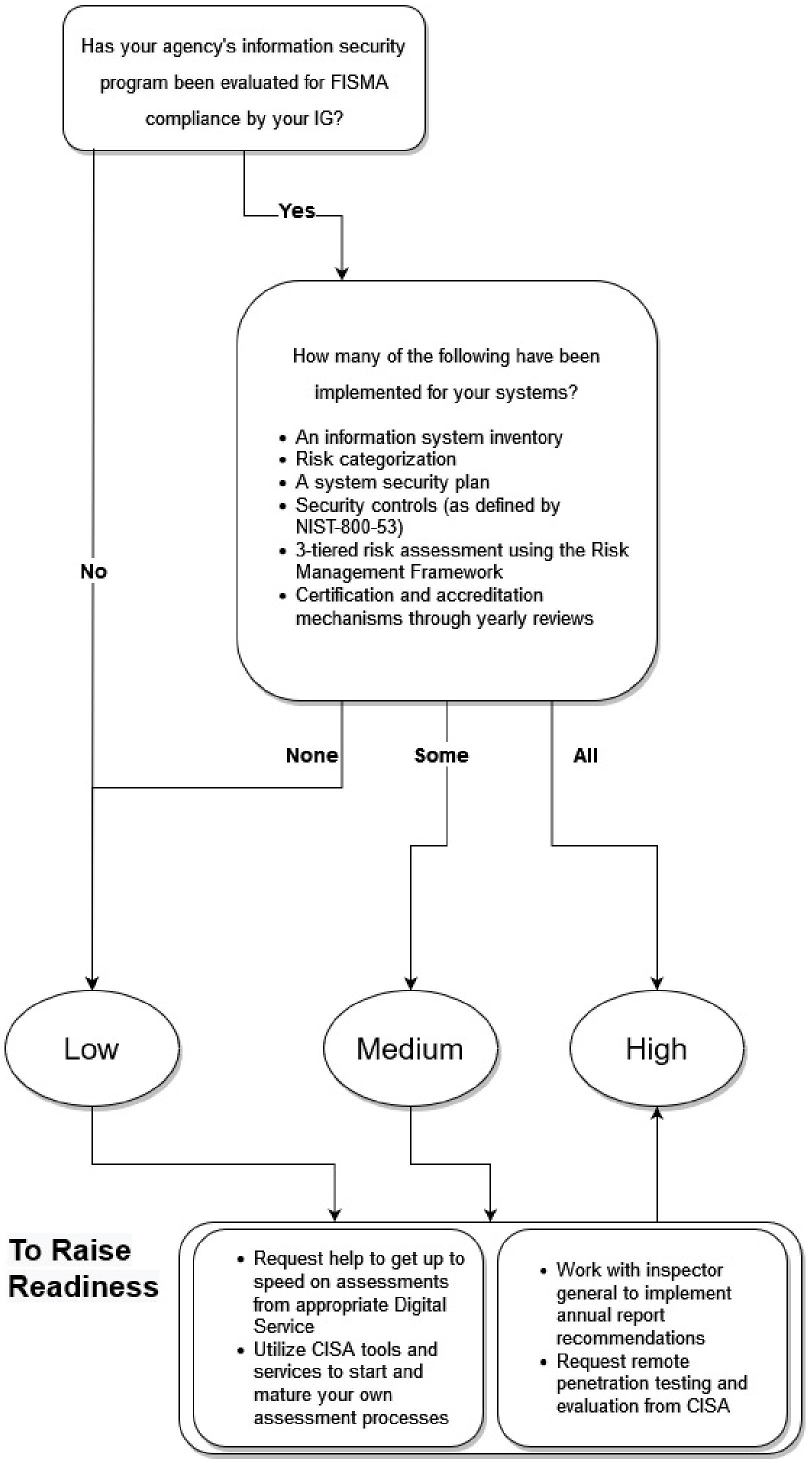
- Remediation of **critical** vulnerabilities within 15 calendar days of initial notification
- Remediation of **high** vulnerabilities within 30 calendar days of initial notification
- Remediation plan if no resolution within specified time frame
- Tracking reports
- Internal coordination (with those who need to know)
- Process for triage, prioritization, and resolution development
- Handling for reports out of scope
- Management of communications with vulnerability reporter
- Evaluation of potential previously unknown impacts
- Procedures around federal incident reporting

To Raise Readiness

- Follow GSA's **public disclosure of vulnerabilities** example to craft your handling policy
- Designate a **technical POC** to communicate with CISA about **cyber hygiene scanning** access

- Publish a vulnerability management procedure for your team
- Hire or outsource staff to handle high and critical vulnerabilities

Security Assessment Readiness



Has your agency's information security program been evaluated for FISMA compliance by your IG?

How many of the following have been implemented for your systems?

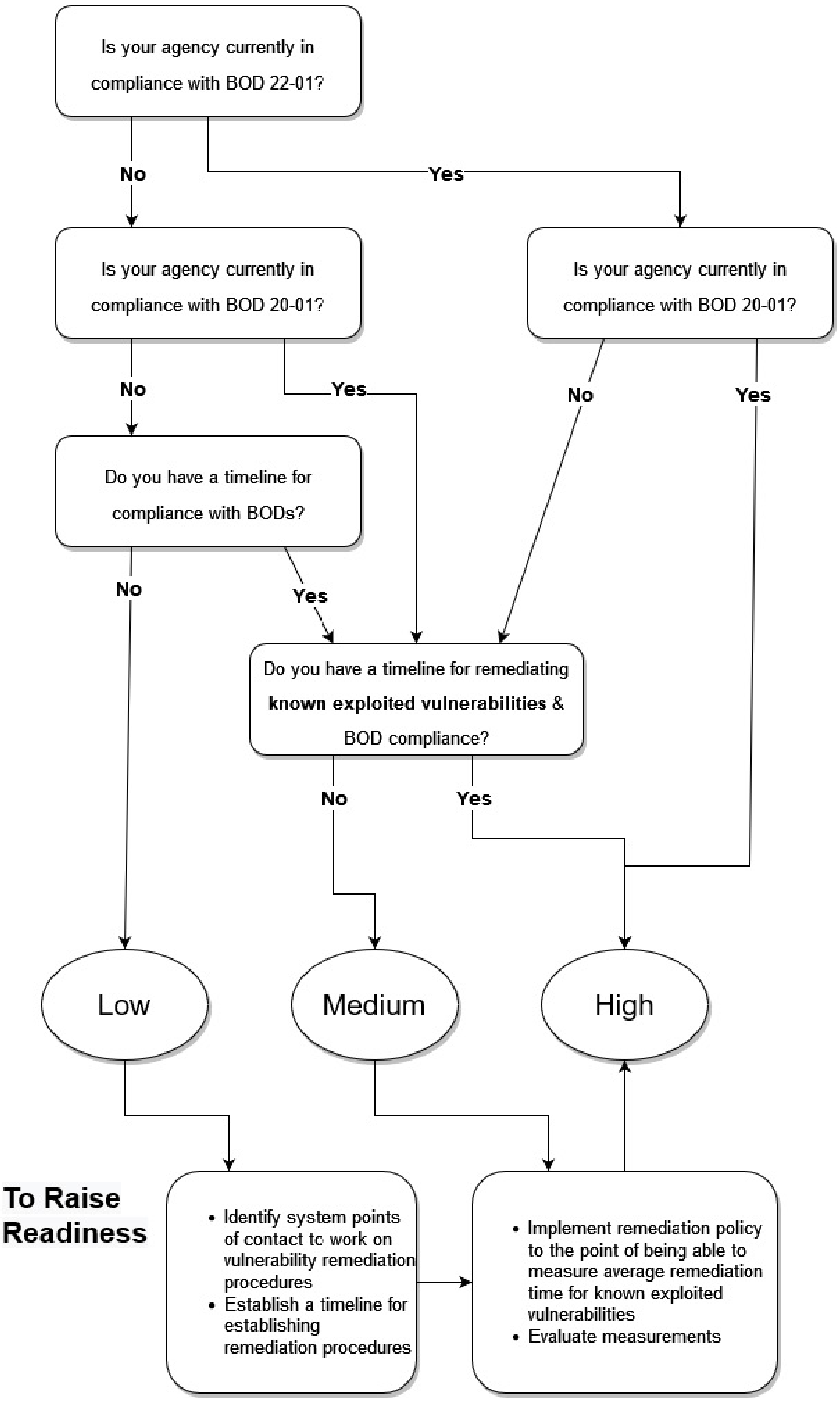
- An information system inventory
- Risk categorization
- A system security plan
- Security controls (as defined by NIST-800-53)
- 3-tiered risk assessment using the Risk Management Framework
- Certification and accreditation mechanisms through yearly reviews

To Raise Readiness

- Request help to get up to speed on assessments from appropriate Digital Service
- Utilize CISA tools and services to start and mature your own assessment processes

- Work with inspector general to implement annual report recommendations
- Request remote penetration testing and evaluation from CISA

Backlog Management Readiness


Is your agency currently in compliance with BOD 22-01?
No
Yes
Is your agency currently in compliance with BOD 20-01?
Is your agency currently in compliance with BOD 20-01?
No
Yes
No
Yes
Do you have a timeline for compliance with BODs?
No
Yes
Do you have a timeline for remediating **known exploited vulnerabilities** & BOD compliance?
No
Yes
Low
Medium
High
To Raise Readiness

- Identify system points of contact to work on vulnerability remediation procedures
- Establish a timeline for establishing remediation procedures

- Implement remediation policy to the point of being able to measure average remediation time for known exploited vulnerabilities
- Evaluate measurements

Tech Policy Primer

BUG BOUNTY PROGRAM READINESS SCORE GUIDE

aspen institute