Life Insurance Association Singapore
LIFE IS WORTH PROTECTING. INVEST IN IT.

GENERAL INSURANCE ASSOCIATION

Bug Bounty Guidelines (Insurance)

By *Insurance Standing Committee for Cyber Security (ISCCS)*

11 October 2021

Change History

Version	Change Description	by	Date
1.0	Initial Official release	ISCCS	11 October 2021

Table of Contents

1. Executive Summary

1.1 Overview

A bug bounty program (BBP) is a crowdsourcing initiative that rewards individuals for discovering and reporting software bugs. It is typically initiated by a sponsoring organisation, enlisting the assistance of bug bounty platforms to manage the program with the organisation. BBPs are often initiated to supplement other forms of security assessments, such as:

- Penetration tests
- Vulnerability scans
- Source code security review
- Static application security testing (SAST)
- Dynamic application security testing (DAST)

1.2 Objectives of BBPs

BBPs are useful to achieve the following objectives for an organisation:

- Uncover security vulnerabilities as supplement to other vulnerability management activities, as highlighted in 1.1
- Pooling together a larger and diverse pool of security researchers and ethical hackers to further mitigate the risk of possible security or data leakage incidents
- Validate the organisation's cybersecurity maturity

This document is intended to provide the insurance community operating in Singapore with a fundamental understanding of the guiding principles and methodology that can be adopted in planning, preparing, executing and closing off a BBP.

2. Introduction

2.1 Intent and Purpose of Guidelines

This set of guidelines serves as a reference to all member insurers of Life Insurance Association (LIA) and General Insurance Association (GIA), who are planning to embark on the journey of a BBP for their organisation. It provides key recommendations on the planning and implementation of a typical BBP for the insurance industry, and may serve as an informal guide for member insurers to be aligned on the expectations of the scope and scale of a typical BBP.

This document is not meant to substitute for, or to supersede, any existing or future corporate, national or regulatory requirements relating to the conduct of BBPs.

2.2 Role of BBP

BBP is a form of security testing that requires sufficient resources, governance and authority to execute effectively. It is meant to provide an alternate approach to discover software security bugs by providing rewards to security researchers and ethical hackers who have contributed to the discovery of the bugs. The rewards are commonly known as bounties, and the bounties paid out should be commensurate with the severity of detected security bugs, the size of the organisation’s IT environment, the difficulty in penetrating the system, as well as the extent of impact the bug would potentially have on the business should it have been exploited.

In practice, a BBP should not be treated as a complete substitute of other security assessment and tests, such as secure code reviews and penetration testing. Rather, it should be used to supplement an organisation's vulnerability management strategy in continuous enhancement of the overall information security posture.

Monetary Authority of Singapore (MAS) in Technology Risk Management Guidelines (TRMG) dated Jan 2021 has also recommended that FI may consider conducting a BBP to test the security of its IT infrastructure to complement its Penetration Tests.

2.3 Key Comparisons

BBPs differ from other forms of security assessment and testing techniques in terms of the goals and methodologies. Many security professionals tend to draw comparisons between penetration tests and BBPs, but there are differences between both testing methods. The following table illustrates the key differences between a BBP and the typical penetration test.

	BBP	**Penetration Test**
Scale	Access to large number of security researchers	Limited to a small group of security consultants
Reporting of Results	Mainly report of the findings discovered and recommendations, with not much information on the approach and objectives.	Usually concluded with a report that state the pre-defined approach, objectives, timeframe and reasonable assurance on the test outcome.
Competitiveness	Very competitive environment. The one who reports a bug first gets the rewards	Not exposed to a competitive environment, which can affect the quality and depth of work
Incentive / Pricing	Pay Per Bug (PPB) model, i.e. incentivised based on *quality* and *severity* of bugs found Engagement fee is based on total payout reward to the individual who	Pay per report, i.e. incentivised by specific engagement with customer Engagement fee is usually fixed, based on man day rate charges by

	BBP	Penetration Test
	discover the vulnerability, variable amount depends on the risk severity and the scope of the affected modules.	security firm and maximum testing duration.
Primary Objective	Primary objective is to identify high value vulnerabilities, with the support from subject matter expert to exploit the system in depth, under a longer timeframe (e.g. 1 month) and a large number of hunters (e.g. more than 10 person).	Primary objective is to identify as many vulnerabilities as possible, under a limited timeframe (e.g. 1-2 weeks) and limited number of testers (e.g. 1-2 person).
Location and accreditation of Testers	Hunters are located in different legal jurisdiction and may not be bounded to any contractual agreement with FI other than the BBP service provider. No requirement to be accredited or certified and only require the domain expertise knowledge and be well-equipped with the relevant tools.	Testers abide by contractual obligation in the service-level-agreement established with security consulting firm that are typically accredited or certified, e.g. CREST.
Remediation	Remediation of findings are based on the risk management framework of the FI. May be treated with higher priority due to the nature of BBP to source for high value vulnerabilities with direct impact to production and assessed to have higher risk severity.	Remediation of findings are based on the risk management framework of the FI.

3. Benefits of Bug Bounty Program

BBP has been widely adopted by organisations globally to improve Information Security posture continuously because of the following benefits:

3.1 Access to potentially wider talent pools

In a typical penetration testing engagement, organisations would have certain headcounts (constrained by budget) to assess the security of their IT infrastructure and applications. For BBP, as more bug bounty hunters would typically be involved in the program, it increases the likelihood of finding more vulnerabilities. Additionally, the bug bounty hunters also have different range of specialised expertise and experiences from their participation in various BBPs.

3.2 Enhance speed of detection and remediation

A bigger group of bug bounty hunters may enable the organisation to discover vulnerabilities before the cyber attackers discover it. In other words, running BBP may allow organisations to get ahead of the attackers by being proactive. Detected vulnerabilities can be remediated right away after they are discovered.

3.3 Develop culture of continuous security enhancement

BBP develops the skillsets of cyber defenders within the organisation and helps them to keep pace with real-world cyber security threats since detected vulnerabilities must be either remediated or mitigated in a prompt manner. It serves as a constant reminder that organisations must always stay up-to-date with latest security landscape.

3.4 Cost-effective

Organisations only pay for validated vulnerabilities, not simply for the efforts of the white hackers since BBP platforms only reward the bug bounty hunters when the vulnerabilities are proven valid. This works slightly differently from penetration testing where the fee will need to be paid regardless of whether vulnerabilities are discovered.

4. Getting Started

a. FI should first ensure that it has a security testing program that is already well established and conducted regularly, such as annual penetration test of Internet facing applications and regular vulnerability scans. BBP can then be incorporated into the security testing program of an FI as the next step to enhance its program's maturity level.

b. It is important to be aware of the differences between BBP and other types of security testing. For example, the participants of BBP could be individuals located in different legal jurisdictions and may not be bounded to any contractual agreement with FI, other than with the BBP provider. BBP provider could only offer minimal assurance of their intent and will not hold full responsibility for any rogue behaviour. There is also no requirement for participants to be accredited or certified in security testing. FI should take into consideration the FI's risk appetite, and various operational and legal considerations in organizing such program.

c. BBP also rewards the participants based on the vulnerability that they discover and the severity of the finding. As the monetary reward is not fixed and may vary depending on individual judgement during assessment of vulnerability severity / risk, FIs that are not experienced in running such program may require a BBP provider to provide the assessment.

d. FIs are therefore advised to engage an experienced service provider to manage the BBP for them, including the recruitment of bug bounty hunters and vetting for their background, reputation and country origin. The provider can also assist in program coordination, monitoring the participation rate, and communicating with the hunters. They may also provide an online platform to facilitate communication, to supervise the program progression, track consensus of the risk severity after validation of vulnerabilities, and manage the bounty reward pool, including the disbursement of payout reward.

5. Guiding Principles / Framework

a. FI should consider starting the program with internet-facing applications that are not critical to their business operations, and then plan to expand the program's coverage in subsequent iterations, learning from the experience gained.

b. FI should consider conducting one round of security testing (e.g. penetration test) of the systems identified to be in scope for Bug Bounty, to ensure most of the common security vulnerabilities are remediated before the Program starts. Alternatively, FI may also consider setting up a vulnerability disclosure policy that welcomes bugs reported by public on a goodwill basis.

c. FI should state clearly the scope of the testing, e.g. the exact URLs, and the types of testing that are disallowed or where reward is not payable, e.g. denial of service attack, informational type of findings, or findings that are already known by the FI from its own security testing.

d. FI should have security monitoring arrangement and incident response framework in place, monitor the conduct of the BBP closely, and be ready to respond in the event that the testing leads to a service disruption of security incident.

e. FI should decide if its perimeter defense such as Network Intrusion Prevention system and Web Application Firewall should be excluded from the scope based on the objective of the FI in conducting the BBP.

f. FI should follow its vulnerability remediation framework to ensure that the vulnerability discovered from BBP are remediated timely. Commitment from FI's management and stakeholders such as application owners and custodians should also be obtained to remediate the vulnerability with higher priority, as the vulnerability could be discovered by multiple individuals and made known to the public due to the nature of the program.

g. FI should communicate both its total budget for payouts and the reward for each level of vulnerability severity to the service provider. FI may wish to seek consultation from internal Finance department on matters of taxation such as withholding tax, due to the engagement of hunters that could be from foreign countries.

h. The following table provides some recommendations on establishing a BBP based upon the FI's maturity and experience in conducting a BBP:

FI’s Experience in BBP	Recommended Approach
No experience	- Engage an experienced service provider to manage the BBP - Run the bug bounty as a private (i.e. on an invitational basis only) and time-bound program - Request that the background of the hunters is vetted by the service provider to ensure they are reputable - Select not more than 5 internet websites / applications to be tested, to manage the scope - Conduct the testing using a “black box” approach, with no login credentials given to participants, to manage the impact of the testing.
1-2 years’ experience	- Engage an experienced service provider to manage the BBP - Run the BBP regularly as a private (i.e. on an invitational basis only) and time-bound program - Request that the background of the hunters is vetted by the service provider to ensure they are reputable - Select between 5-10 internet websites / applications to be tested - Conduct the testing using a “black box” approach, with no login credentials given to participants but allow for creation of login accounts by participants, to manage the impact of the testing. - Consider running the Program annually
More than 2 years’ experience	- Engage an experienced service provider to manage the BBP, or FI may consider running the program on its own. - Run the BBP as organisation wide vulnerability disclosure program, i.e. offers reward to individual who reports valid vulnerability regardless of where the vulnerability resides. - Run the bug bounty as a private program, or as a public program with larger number of participants - Request that the background of the hunters is vetted by the service provider to ensure they are reputable (for private program) - Select all internet websites / applications to be tested - Conduct the testing using a “grey box” approach, with login credentials given to participants, but also allow for creation of login accounts by participants - Consider running the program continuously throughout the entire year

6. Methodology

Organisations conducting BBPs are recommended to follow these 4 phases:

1. Planning
2. Preparation
3. Execution
4. Closure

6.1 Planning

6.1.1 Develop Policy and Processes

Work with stakeholders to develop a vulnerability disclosure policy (for public BBP), processes for handling vulnerability reports, and a communication plan for internal and external stakeholders.

6.1.2 Bug Bounty Platform Vendor Selection

Carry out Third Party risk assessment in selecting external vendors and platform to run the BBP. The scope of assessment could include areas such as Security, Data Privacy, Operational Risk, Legal Risk and Business Continuity. Additionally, below are some other considerations in selecting the right platform for the organisation:

S/N	Suggested Requirements
1	Platform capable of running private, public and one-off engagement
2	Bug Hunters have to agree to Vulnerability Disclosure Policy prior to participating
3	Reward Bug Hunter only upon verification, remediation and approval of vulnerability report
4	Provide flexibility of managed services, e.g. the provider manage the program end-to-end or provide an option to clients to choose the services to be provided.
5	Supports API access to data for integrating, importation, correlation with other vulnerability disclosure sources
6	Supports VPN option (require Bug Hunter to be connected to VPN to search for vulnerabilities)
7	Platform restricts access to only users that need access to this program
8	Availability of a program manager to assist in any campaign run at local timing
9	Bug Bounty reporting, metric, alerting and analytics
10	Support for Black, Grey and white box testing
11	Secure submission forms that let hunters disclose vulnerabilities to organisations privately
12	Support Multi-Party Coordination
13	Large number of Bug Hunters behind the platform

S/N	Suggested Requirements
14	Competitiveness of pricing
15	Quality of Bug Hunters and experience of the platform vendor
16	Ability to mobilise local Bug Hunters
17	Ease of tracking issues on the platform and flexibility to integrate with company's IT Service Management (ITSM) tool
18	Certification and compliance considerations like GDPR, ISO27K, ISO 29147, if applicable
19	Total number of public and private program ran till date
20	Number of active public bug bounty companies and published names
21	Has control on which hackers are invited and who is eventually approved to participate in public (if available) and private program.
22	Allow for custom requirements i.e. NDAs, background checks of Bug Hunters.

Organisations can also consider getting the vendors to conduct demonstrations of their platforms and assess how each vendor meets the requirements.

6.1.3 Engage the Right Team and Communicate to those that need to know

It takes a team of multiple subject matter experts to deliver a successful BBP. Organisations can consider using a RACI (responsible, accountable, consult, and inform) matrix to define the roles and responsibility of the multi-disciplinary teams. Other than the IT security and software development teams, other stakeholders that should be considered include:

Legal: Companies that implement a BBP should ensure the involvement of a legal team. Legal issues that tend to come up may include: liability if a Bug Hunter exploits an application vulnerability and access sensitive information such as customer's personally identifying information (PII); a Bug Hunter publicly disclosing a vulnerability before it is fixed; Know Your Customer (KYC) anti-money laundering laws; and Bug Hunters who might be in locations where the US has active sanctions.

Corporate Comms. For public BBPs, it is recommended to include the corporate communications teams to ensure they give input on the verbiage and branding being used, and prepare "drawer statements" prior to the commencement of the exercise.

A sample RACI is set out in the appendix of this document.

For organisations that undertake BBP for the first time, the BBP team may find themselves inundated with messages and queries from internal teams. Agreeing on a certain set of communication channels and protocols will align everyone's expectations and reduce the noise that may interfere with the conduct of the BBP. Additionally, one good practice that can accelerate the resolution time of vulnerabilities is to include both the triage and software development teams in the same communication channel so that the latter can pre-emptively start on the solutioning.

6.1.4 Practice Drill

Organisation may consider running a Table top exercise as a way to familiarise staff on the roles and responsibilities, escalation procedures, and processes during the BBP.

6.1.5 Considerations on various setups of Bug Bounty

There are various considerations that need to be decided in order to deliver a successful bug bounty suited for your company

6.1.5.1 Black Box vs Grey Box

- Black Box: Performed without any prior knowledge and access to the environment, like if you were attacked by an offshore hacker.
- Grey Box: A hybrid type of black and white box testing to simulate an attacker that has already compromised some security measures.

Black box testing offers the organization a good sense of the security posture of the application to withstand attacks from external threats, especially threats that have no inside knowledge of the application. However, it does not uncover all vulnerability that could still be present in the application and potentially be exploited. With Black box testing, the over-all vulnerability that will be detected will depend on the scope and the skills of the bug hunters.

Grey box testing approach will provide more assurance that the application is tested in depth and to discover as many vulnerabilities as possible. However, the testing could be intrusive and may result in alteration of data in the application, or disruption of service.

Recommended practice is to go with black box testing first where the bug hunters need to find ways and means to break through the application. The organisation can monitor the progress and then transit into grey box testing where credentials can be provided to the hunters for them to login and access deeper into the application, and to widen their testing scope.

6.1.5.2 VPN vs Direct

Usually, the Bug Bounty Platform will make available a VPN option for Bug Hunters to connect. This will make the it easier to whitelist the IP addresses to identify legitimate traffic directed towards your application that is planned for bug bounty.

If the IP address is not whitelisted, the attack traffic from the Bug Hunter may not even reach the intended system as the perimeter security controls may have already prevented the attack.

The decision on whether to require Bug Hunters to connect to the VPN depends on the engagement model and scope of the bug bounty, and whether the objective is to test the intended application, capability of the perimeter control, or both.

Experience shows that some Bug Hunters are not very keen to connect to VPN as there are ways to track and log their activities while they are ploughing their trade. Requiring that all Bug Hunters must connect to VPN to search for vulnerabilities could thus reduce the number of Bug Hunters participating in the BBP.

Additionally, security measures should also be in place (e.g. access control, network segregation, etc.) when exposing internal network connectivity via VPN, as access credentials could be shared beyond the authorised BBP hunters.

6.1.5.3 In-scope vs Out of scope – Testing and Bugs

The scope needs to be clearly defined, such as the websites that are in and out of scope. The bounty will only be applicable to bugs found in websites that are in scope.

Some very common scoping questions to guide you include:

- What does your application consist of? Web, Mobile, IoT?
- What assets do you wish to test? Be specific. For example, there is a big difference between myapp.com and *.myapp.com
- Have you defined what bugs are Out of Scope? It could be known issues, intended functionality, low hanging discoveries, accepted risks, or findings that are similar or derivatives of other findings.

  Other examples of non-qualifying vulnerabilities include:

  - Issues related to 3rd party or Commercial Off-The-Shelf (COTS) products or websites not under the organisation’s control
  - Social engineering attempts including phishing emails
  - Brute force attacks
  - Spamming
  - Exploitation beyond what is minimally required to prove a web vulnerability exist. E.g. defacement
  - Distributed Denial of service (DDoS)
  - Recently disclosed 0-day vulnerabilities
  - Prior Pentest findings

- Do you allow testing that may disrupt your production application services to customers? Most bug bounty testing would specifically exclude techniques that overwhelm the network infrastructure such as DDoS, or brute-force guessing of login passwords that may cause account lockouts.

- Are there any external systems that are Out of Scope? For example, Identity and Access Management (IAM), SSO, 3rd party systems that you're integrating with, internal dev tools and services (code repository, DevOps tools etc.)

6.1.5.4 Private vs Public Programs

BBPs can be run as public or private engagements. Historically, the only way to conduct a bug program was by publicly announcing it. With the increasing popularity of bug bounty platforms used by large pools of security Bug Hunters, it is now possible to exclusively invite a small subset of those Bug Hunters to participate in a private program.

- **Public or On-going**. A public BBP is announced publicly, generally published to the public Internet and is available for anyone to participate. They also come with the benefit of marketing an organisation's information security program, indicating to customers and partners that security is a priority. These are typically long-term, continuous reward programs that incentivise Bug Hunters to uncover vulnerabilities.
- **Private or Time-bound.** Private BBPs are by invitation. They are opened only to selected group of known Bug Hunters with good track records of not straying out of the testing scope and following program rules. Such Bug Hunters reduce some of the risk factors of doing a BBP. This is best for limited budget or short-term needs or for those that started exploring bug bounty. Such invitation-only programs usually last between two to four weeks

6.1.5.5 Managed Service vs Non-Managed Service

Non managed Service

Basic advisory service will be provided. There will typically be limited interaction with the BBP provider, and the services provided tend to cover the following only.

- Review the scope together to define the rules and rewards grid.
- Select bug hunters according to the organisation's scope and needs.
- Help define reward grids in line with the organisation's maturity/complexity and budget to keep the program attractive.

FIs should also ensure the internal teams have adequate skillsets to manage the program, such as knowledge in application security findings to be able to triage the vulnerability, and security monitoring capability to monitor the attempts of the hunters.

Managed Service

Managed services typically provide customers the ability to: onboard, launch, and scale BBPs, connect and maintain healthy relationships with Bug Hunters, validate and manage incoming vulnerability reports, and pay Bug Hunters.

The platform will usually provide the following resources: A Program Manager for expediting program on-boarding and launching coordination, and resources to support Bug Hunter management and deployment, validating incoming vulnerabilities, and provide in-program performance management.

Managed service is recommended for those that need support in familiarising with the bug bounty platform and those that are new to the Bug Bounty engagement. The managed services scope will usually include:

- Analysing the vulnerability discovered.
- Verifying the validity of this vulnerability with respect to the rules of the given program.
- Checking whether the vulnerability had been previously reported.
- Determining the severity level in consultation with the client (i.e. editing CVSS score or CWE if necessary).
- Adding technical elements or fixing advice to facilitate the work of the software development team.
- Handle payment of the corresponding reward, after approval from the client.
- Manage interactions needed to process the Bug Hunter's report.

6.1.5.6 Curated, Local hunters vs any hunters in the platform

Usually, private bug bounty will allow the company to have access to a curated list of Bug Hunters so that the company can exercise additional due diligence over the bug hunters e.g. ranking, country of residence, track records etc. to be invited for the private bug bounty engagement.

As for public bug bounty, it will be an open invitation to the Bug Hunters that have an account with the platform.

6.2 Preparation

An important prerequisite for embarking on a BBP is **having a strong Vulnerability Management and Incident Response (IR) plan**. It is crucial to enable quick and coordinated response to the reported vulnerabilities, or if the testing results in an incident.

6.2.1. Environment Preparation

- Identify the appropriate environment for the bug bounty engagement.
- Depending on your testing approach e.g. Black box, Grey box or Black box and progressively to Grey box, provision the necessary accounts/credentials for your bounty hunters to use.
- Ensure that there are monitoring and logging in place to verify any deviations from the scope, and ensure program rules are adhered to.
- If your BBP is private where participation is more exclusive, do whitelist any IPs and manage any firewall settings necessary for the Bug Hunters' participation.

- Anticipate where are the potential choke points which will stop the Bug Hunters from doing their work. It is especially frustrating to the Bug Hunters if the organisation needs to pause the program repeatedly due to various issues such as system cannot handle too much traffic, or the WAF / IPS kicks in and blocks the attack.
- Communicate to the "Defenders" of the company of such activity to avoid false alarm.
- Communicate to IT and development teams to be prepared to react to vulnerabilities reported and to resolve them accordingly based on the severity.
- Business units that owned the application and dependent process and systems need to be informed of the activity as well.
- For public program, it is good to keep the entire company abreast of such activity as it's an open invitation for Bug Hunters to openly attack our application on a long term basis.

6.2.2. Reward and paying bounties

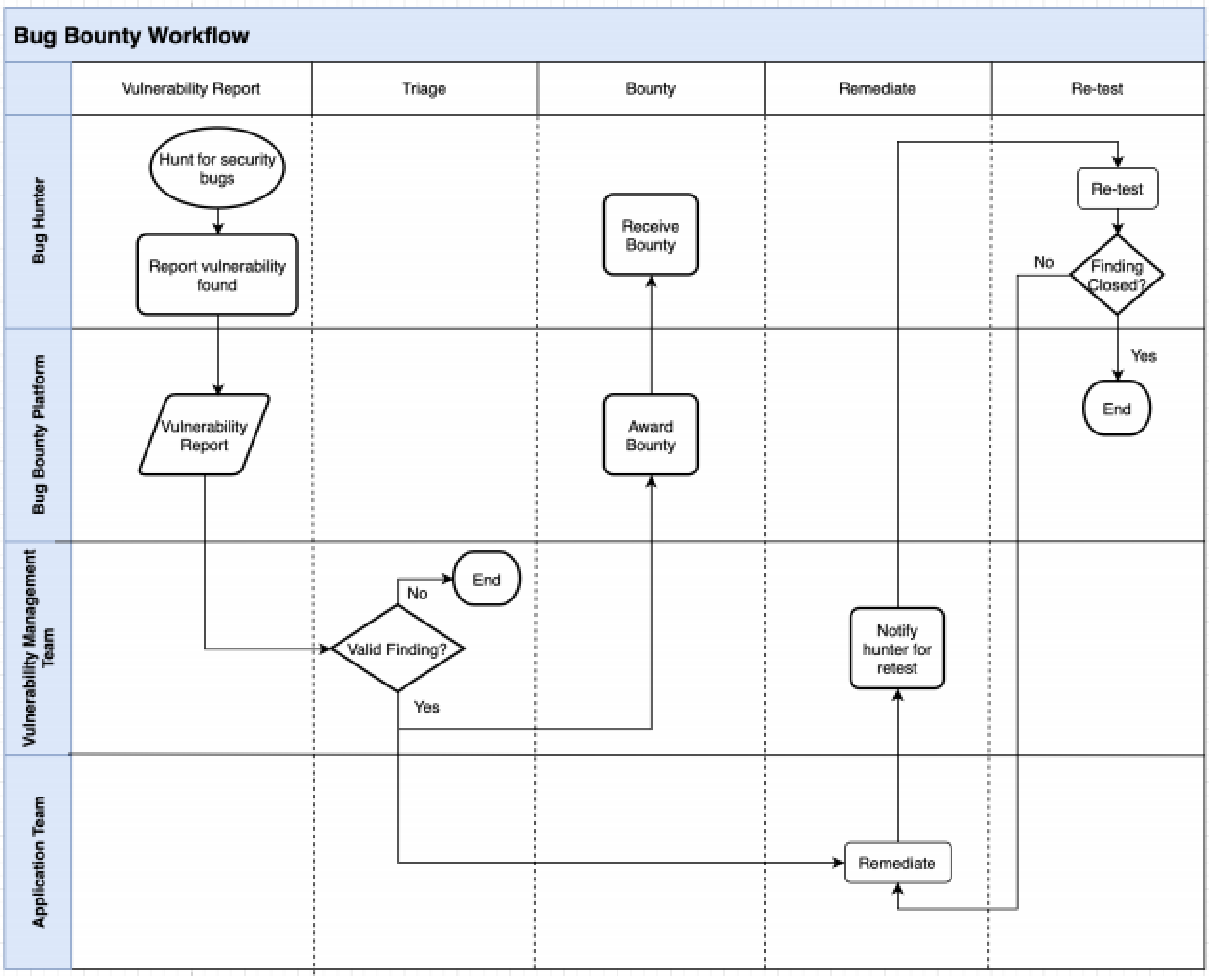
Initially a program could possibly pay out a range of bounty for low, medium, high, and critical bugs respectively. Over time, the applications will be more secure and vulnerabilities would become harder to find. As time passes, bug submissions tend to drop and increasing the rewards keeps Bug Hunters' interest high. If Bug Hunters must spend more time discovering vulnerabilities against a hardened application, the incentives have to be adjusted.

6.3 Execution

With all the considerations deliberated and updated in the platform, the BBP is ready to commence. Assuming the organisation decided to engage a BBP managed service provider, there should be close interaction with the Program manager especially at the start of the program. Organisation should also have regular catch-up with the Platform Program Manager, e.g. daily, at the first few weeks of the program. This will enable the organisation to clarify queries, review the vulnerability reports reported, make changes to the BBP where necessary, and plan for the next steps.

During the actual bounty hunting period, the pace of the incoming reports will not always peak at 100%. In the beginning, organisation should be prepared to respond to more reports of vulnerabilities especially during the weekend period where activities tend to be higher. As time goes by, the reports will drop as more valuable findings are reported first. Another possible resurgence could happen if there is an increase in the bounty amount which naturally rejuvenates the interest of the bounty hunters.

A sample workflow of the execution of BBP is set out below:



6.3.1. Vulnerability Report

Bug Hunters will interact with the bug bounty platform to submit a vulnerability report. Minimally a good report requires the following:

- A comprehensive description of the issue
- Detailed step-by-step instructions on how to reproduce it
- A clear impact analysis that justifies the severity of the report
- Report of Bugs – verifiable proof that the vulnerability exists (e.g. screenshot, video, script or proof of concept) with sufficient information about the detected vulnerabilities.
- Examples to include:
  - URL and/or IP address of the affected system
  - Date & Time of access (timestamp)
  - Product, version and configuration of the software containing the bug
  - Impact of the issue
  - Suggested mitigation or remediation actions if any.

6.3.2 Triage

The BBP managed service provider (depending on whether you are subscribed to managed services) works on the triage queue analysing each report, assessing the application with the potential issue, and determining if the vulnerability is valid.

6.3.2.1 Bounty

When it has been determined that the Bug Hunter has submitted a valid vulnerability, they can be paid the appropriate amount that is commensurate with the criticality of the vulnerability through the bug bounty platform. Bounty payments typically happen either after the vulnerability is triaged and confirmed, or after it is fixed.

6.3.2.2 Remediation

The internal remediation process will typically be similar to the remediation process for application vulnerabilities identified during other forms of security testing e.g. penetration testing. However, due to the nature of an externally reported security issue, the risk and prioritisation might need to be higher than vulnerabilities identified during other forms of internal testing.

After the fix is deployed, depending on the service subscribed, the BBP vendor or Bug hunters may assist to re-test the application to ensure that the vulnerability is remediated.

6.4 Closure

6.4.1 Access termination

All provisioned access should cease on the stipulated end date and time.

6.4.2 Reporting

Depending on the service subscribed, the BBP platform vendor may provide a formal report to summarise the findings and conclusion of the testing.

It will be good if BBP service provider can provide a summary of the security test cases conducted by the hunters with reference to industry standards such as OWASP Top Ten Web Vulnerability.

6.4.3 BBP Review and Lessons Learned

At least after one cycle, it is beneficial to look into how the BBP can further improved by considering the following items:

- Budget
- Number of Reports
- Reports Quality
- Rewards Matrix
- Findings Validation and Severity Calculations
- Remediations and Retesting

7. Appendix

7.1 Acronyms, Terms & Definitions

Terms	Definitions
SAST	Static application security testing, or static analysis, is a testing methodology that analyses source code to find security vulnerabilities that make your organisation's applications susceptible to attack. SAST scans an application before the code is compiled.
DAST	Dynamic application security testing looks for security vulnerabilities by simulating external attacks on an application while the application is running. It attempts to penetrate an application from the outside by checking its exposed interfaces for vulnerabilities and flaws.
MAS	MAS is the central bank of Singapore. MAS oversees every aspect of monetary policy, banking and finance in Singapore, including matters relating to the insurance industry. According to its mandate, MAS' role as central bank involves: Conducting monetary policy, including issuing currency and overseeing payment systems.
CREST	The Council for Registered Ethical Security Testers. CREST provides internationally recognised accreditations for organisations and professional level certifications for individuals providing penetration testing, cyber incident response, threat intelligence and Security Operations Centre (SOC) services.
BBP	A bug bounty program is a deal offered by many websites, organisations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.
CVSS	Common Vulnerability Scoring System is an open framework for communicating the characteristics and severity of software vulnerabilities.
CVE	Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that's been assigned a CVE ID number.
CWE	Common Weakness Enumeration is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.
FI	Financial Institutions
WAF	A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.
IPS	An intrusion prevention system (IPS) is a form of network security that works to detect and prevent identified threats. Intrusion prevention

Terms	Definitions
	systems continuously monitor your network, looking for possible malicious incidents and capturing information about them.
RACI	RACI is an acronym that stands for responsible, accountable, consulted and informed. A RACI chart is a matrix of all the activities or decision making authorities undertaken in an organisation set against all the people or roles.
Penetration tests / penetration testing	Security evaluation of targeted infrastructures or applications to identify security vulnerabilities within a defined timeline with indicated start date and end date.
Vulnerability scans	Automated tools that allow organisations to verify their infrastructure and applications of any known security vulnerabilities
Source code security reviews	Manual or automated review of an application source code in an attempt to identify security weaknesses (flaws) in the code
VDP	Vulnerability Disclosure Page, a webpage for hunters to report bugs.
BBP platforms / providers	Organisations that provide crowd-sourced security services by connecting their customers / potential customers with white-hat bug bounty hunters / security researchers as the main business model. The platforms allow bug bounty hunters / security researchers to perform security evaluation of the customers' Information Security postures according to the defined set of rules.
Bug bounty hunters / security researchers	Individual engaged by BBP platforms / providers to perform security evaluation of the customers' Information Security postures according to the defined set of rules

7.2 Checklist for Bug Bounty program

No	Activity	(Completed/In-Progress/Blocker/Not required)	Comment
1	Assess the business need for a BBP		
2	Be aware of the differences between BBP and other types of security testing, including the role of the BBP provider.		
3	FI should consider conducting one round of security testing (e.g. penetration test) of the systems identified to be in scope for Bug Bounty, to ensure most of the common security vulnerabilities are remediated before the Program starts		
4	Develop Policy and Processes, (see 6.1.1)		
5	Select Bug Bounty Platform Vendor Selection (see 6.1.2)		
6	Define RACI and Engage (see 6.1.3, 7.3)		
7	Define Scope and Out-of-Scope (see 6.1.5.3)		
8	Consider Testing Approach and BBP Flow. Document it. (see 6.1.5, 6.2.2, 6.3))		
9	Conduct Table Top Exercise (see 6.1.4)		
10	Prepare the Environment (see 6.2, 6.2.1)		
11	Finalise the Rewards Matrix (see 6.2.2)		
12	*Finalise Program Duration, Reporting and Triage (see 6.3, 6.4)*		
13	*Review the BBP Life Cycle for Continuous Improvements (see 6.4)*		

7.3 Sample RACI for Bug Bounty program

Action	Bug Hunters	Bug Bounty Platform & Program Manager	Security Team	IT / App team	Business App / impacted Business App owner	Legal	Corporate Comms	Senior Management
Provision Bug Bounty Platform		R/A	I					
Inform Internal stakeholder			R/A	I	I	I	I	
Vendor Assessment, Selection / Agreement vetting			R/A	I	C	C		
Incident Management		I	R	C	C	C	C	A/ R
Create Program		R/ C	R/A	I				
Refill wallet		R/C	R/A					
Set Reward award		R/C	R/A					
Set Program Rule		R/C	R/A					
Invite Hunters		A/R	C/I					
Sign up BBP	A/R	R						
Vulnerabilities reporting	A/R	I	I					
Triage vulnerabilities reported		A (if managed services) / R	A (if not managed services) / R	I	I			
Inform Internal app regarding valid finding		C	A/R	I				
Remediate vulnerabilities		I	C	A/R	I/C			
Verify the fix of vulnerability	R	I	A	I/C	I			
Release award to hunter	I	I	A/R					