bugcrowd

Penetration Testing Services & Compliance Applicability Review

September 2022

Prepared by

schellman

Proprietary & Confidential

Statement of Confidentiality

The purpose of this document is to provide Bugcrowd, Inc. (Bugcrowd) with the results of Schellman's review of Bugcrowd Penetration Tests (Basic, Standard, Plus, and Max tiers) and Managed Bug Bounty services as it relates to the Payment Card Industry Data Security Standard (PCI DSS) and other regulatory and compliance requirements on penetration testing.

This document, and any other Bugcrowd related information provided, shall remain the sole property of Bugcrowd and may not be copied, reproduced, or distributed without the prior written consent of Bugcrowd.

Applicability

The information found in this white paper and the conclusions reached were dependent upon the complete and accurate disclosure of information by Bugcrowd.

QSA Independence Disclosure

Schellman Compliance, LLC. ("Schellman") reviewed certain aspects of the Penetration Test Basic, Penetration Test Standard, Penetration Test Plus, Penetration Test Max, and Managed Bug Bounty services for Bugcrowd from September 6, 2022, through September 9, 2022. During this time, Schellman did not hold any investment or control over Bugcrowd. During the course of this review, Schellman and the QSA did not market services for the purpose of assisting Bugcrowd in meeting any regulatory requirements pertaining to the penetration testing services reviewed as part of this white paper. No Schellman service was recommended during the course of the engagement.

Schellman also performed the System and Organization Controls (SOC) 2 and SOC 3 examinations as well as the ISO 27001 certification review for Bugcrowd prior to the assessment.

TABLE OF CONTENTS

SECTION 1: EXECUTIVE SUMMARY

Purpose

Schellman performed a review of Bugcrowd Penetration Test Basic, Penetration Test Standard, Penetration Test Plus, Penetration Test Max, and Managed Bug Bounty services for alignment with applicable penetration testing requirements of the PCI Data Security Standard v3.2.1, PCI Data Security Standard v4.0, ISO/IEC 27001:2013 (ISO 27001) Annex A, and NIST 800-53 revision 5. This assessment was completed in September 2022 by Schellman Compliance, LLC.

Scope of Work & Approach Taken

Schellman interviewed Bugcrowd personnel via live web-based video conference, and reviewed documentation provided by Bugcrowd. The following Bugcrowd services were included in the review:

- Bugcrowd Penetration Test Basic
- Bugcrowd Penetration Test Standard
- Bugcrowd Penetration Test Plus (formerly "Classic Pen Test")
- Bugcrowd Penetration Test Max (formerly "Next Gen Pen Test")
- Bugcrowd Managed Bug Bounty

Objective

The objective of this assessment was to assist Bugcrowd in validating how the services enable its customers to meet applicable compliance requirements for penetration testing. This assessment specifically targeted the standard agreements and instructions provided to customers as well as a detailed review of standard and customizable reports available to customers

SECTION 1: EXECUTIVE SUMMARY

Company Background & Services Provided

Company Background

Bugcrowd is a Crowdsourced security platform that helps customers infuse the power of the Crowd into all of their security testing initiatives. The platform provides solutions for secure vulnerability disclosure, bug bounties, penetration testing, and attack surface management. Bugcrowd's principal service offerings combine data, technology, and human ingenuity for the rapid identification and reporting of previously unknown attack surface and security vulnerabilities, which are validated, triaged, and prioritized by Bugcrowd. Real-time vulnerability view, and 24/7 reporting are offered via the Bugcrowd customer console for enhanced visibility throughout every engagement. Bugcrowd advocates that a community of highly vetted researchers provides significantly more value than traditional penetration testing services.

Penetration Test Basic

Bugcrowd Penetration Test Basic (PTB) aims to provide a basic vulnerability assessment report based on automated scanning. In this service, an industry-recognized vulnerability scanning tool is run against the customer-provided target list. A Bugcrowd penetration tester then reviews the list of potential vulnerabilities, and verifies each one, including attempting to exploit the vulnerability, in order to eliminate false positives, and identify exploitable vulnerabilities. Findings are combined into a compliance friendly Penetration Test Report. The Basic service is provided on a per-engagement basis: however, a retest can be performed to confirm remediation of vulnerabilities if Bugcrowd's customer purchases an add on to the existing test.

Penetration Test Standard

Bugcrowd Penetration Test Standard (PTS) aims to satisfy requirements from auditors and reviewers in a pay-for-time format that is generally more amenable to certain procurement or budgetary requirements. In this model, Bugcrowd leverages the same global Crowd of talent that is automatically matched and managed for each testing engagement. Unlike the Penetration Test Max service, researchers are not incentivized for findings beyond completion of the standardized methodology. Bugcrowd employees perform the review, validation, and triage for all findings, before combining them into a compliance friendly reporting format. Bugcrowd PTS includes testing of external-facing IP address ranges and web pages, with add-on services, such as internal targets, advanced services and retesting available for an additional cost.

SECTION 1: EXECUTIVE SUMMARY

Penetration Test Plus (formerly “Classic Pen Test”)

Bugcrowd Penetration Test Plus (PTP) aims to satisfy requirements from auditors and reviewers in a pay-for-time format in the same manner as the Standard service. Plus includes all of the services included in Standard, with additional flexibility and customization options available, such as internal targets, different types of targets, including web pages, APIs, mobile applications, cloud-based infrastructure, IoT devices, and retesting.

Penetration Test Max (formerly “Next Gen Pen Test”)

Bugcrowd Penetration Test Max (PTM) aims to encourage greater vulnerability discovery while helping organizations satisfy various regulatory and compliance requirements. In a traditional pay-for-results crowdsourced security program, researchers are incentivized to find vulnerabilities before the competition, which can be at odds with the motivation to follow a comprehensive methodology that requires testing for non-rewardable findings. This can pose issues for companies attempting to leverage a bug bounty program for compliance purposes. Bugcrowd has addressed this issue with Penetration Test Max. In this model, Bugcrowd deploys bounty-incentivized researchers alongside grant-incentivized penetration testers to ensure a defined methodology is completed in full. They accomplish this with the help of their CrowdMatch Skills Selection methodology to identify the proper resource(s) with the appropriate knowledge and demonstrated aptitude for the environment to be tested. Additional service options for Max include premium Service Level Agreements (SLA), and vulnerability retesting. Bugcrowd employees review, validate, and triage findings before combining them into a compliance friendly reporting format. This ensures a repeatable and defensible methodology is followed every time.

Managed Bug Bounty

Bugcrowd Managed Bug Bounty (MBB) programs utilize the same global Crowd of talent used for the other penetration test offerings, except that instead of using a small number of researchers who are paid to follow specific steps in a defined methodology, a larger group of Bug Bounty researchers are incentivized to be the first to find issues. Further, it is up to the tester to determine what areas of the defined scope they want to test, and how much effort they put into the testing. Similar to the other Bugcrowd penetration testing services, the customer defines the scope of what is to be included in the test, provides access and any necessary credentials. Testers agree to rules of engagement and submit vulnerability findings with similar details and evidence as when using one of the prescribed methodologies.

SECTION 1: EXECUTIVE SUMMARY

Summary of Findings

During the review of Bugcrowd Penetration Test Standard, Plus, and Max, Schellman made the following observations that are further explained throughout the rest of this white paper:

- Bugcrowd Penetration Test Standard, Plus, and Max appear to directly assist organizations in meeting the requirements in PCI DSS v3.2.1 Requirement 6.6 for testing public-facing web applications, as well as PCI DSS v4.0 Requirement 6.4.1 until 31 March 2025, when Requirement 6.4.1 will be replaced by Requirement 6.4.2, which removes the option of using manual/automated application testing as the only means to protect web applications for 6.4.x requirements.
- The penetration testing methodology, for Standard, Plus, and Max penetration tests, directly support organizations in achieving compliance with PCI v3.2.1 requirement 11.3 / PCI v4.0 requirement 11.4 for internal and external penetration testing when the customer adequately defines the scope of their environment.
- Bugcrowd Penetration Test Standard, Plus, and Max have the capacity to meet PCI DSS v3.2.1 requirement 11.3.4 and 11.3.4.1 / PCI DSS 11.4.5 and 11.4.6 for network segmentation testing, as long as the customer defines segmentation controls and reviews the results of segmentation testing to determine if the segmentation controls were adequate.
- Bugcrowd Penetration Test Plus and Max have the capacity to meet PCI DSS v4.0 requirement 11.4.5 for isolation controls for separating systems of differing security levels, as long as the customer defines isolation controls and reviews the results of isolation testing to determine if the isolation controls were adequate.
- Schellman reviewed the Standard, Plus, and Max methodologies in collaboration with sample reports and noted that the service offering directly supports NIST 800-53 rev5 CA-8 and ISO 27001 A.12.6.1 requirements for penetration testing.

Although the use of bug bounty programs can assist in identifying vulnerabilities to enhance an organization's information security architecture, on their own they do not provide much assistance in meeting regulatory and compliance requirements.

SECTION 1: EXECUTIVE SUMMARY

During the review of Bugcrowd Penetration Test Basic, Schellman made the following observations that are further explained throughout the rest of this white paper:

- Bugcrowd's Basic offering appears to assist organizations in meeting the requirements in PCI DSS v3.2.1 Requirement 6.6 for testing public-facing web applications, as well as PCI DSS v4.0 Requirement 6.4.1 until 31 March 2025, when Requirement 6.4.1 will be replaced by Requirement 6.4.2, which removes the option of using manual/automated application testing.
- Although the testing methodology used in Bugcrowd Penetration Test Basic can assist in identifying vulnerabilities to enhance an organization's information security architecture, on its own it does not provide much assistance in meeting regulatory and compliance requirements. Notably, Basic does not provide testing of internal targets nor segmentation testing.

During the review of Bugcrowd Managed Bug Bounty, Schellman made the following observations that are further explained throughout the rest of this white paper:

- Bug bounty programs rely on the use of a relatively large number of testers, each of whom specializes in, or self-selects, particular types of testing.
- The overall high-level penetration testing methodology used for Managed Bug Bounty can partially support organizations in achieving compliance with PCI DSS v3.2.1 requirement 11.3 / PCI DSS v4.0 requirement 11.4, if the customer adequately defines the scope of the testing engagement, including ensuring adequate test coverage.

SECTION 2: PENETRATION TESTING METHODOLOGY

Max Penetration Testing Methodology

Alignment with Industry Standards

Schellman observed Bugcrowd's defined testing methodology and noted that it aligned with multiple industry standards for technical testing, including NIST SP 800-115, Web Application Hacker Handbook Methodology (WAHHM), SANS Top 25, Council of Registered Ethical Security Testing (CREST), Open Source Security Testing Methodology Manual (OSSTMM), Web Application Security Consortium (WASC), Penetration Testing Execution Standard (PTES) and the Open Web Application Security Project (OWASP) Testing Guide v4. Review of example penetration testing reports showed that alignment with the aforementioned industry standards was consistent with various regulatory and compliance requirements, such as the PCI DSS v3.2.1, PCI DSS v4.0, NIST 800-53 rev5 and ISO 27001. Further review of the methodology, in conjunction with PCI requirements 6.6 and 11.3, can be found in section three of this white paper. Bugcrowd's methodology for conducting a Max penetration test directly uses the OWASP Testing Guide v4 and its web application security testing steps. Schellman observed example Max reports and noted that each step was included in the testing practices.

Service Options

Bugcrowd's Penetration Test Max service offering includes two options for its customers to choose from; time bound testing and continuous. Time bound testing is done in a manner where the customer chooses the start and end date for which Bugcrowd will conduct the penetration test. All activities conducted by Bugcrowd, and its pool of Crowdsourced researchers are completed during the period identified by the customer. Customers were responsible for ensuring that the time frame of a timebound Max penetration test was adequate to meet various regulatory and compliance requirements.

The continuous testing service is the most commonly chosen delivery format for Max, and provides ongoing testing throughout the year, with methodology-based testing triggered whenever the client specifies. This testing type provides a select subset of researchers and penetration testers controlled, continuous access to the customer's environment. Continuous testing allows customer environments to be tested after significant changes, upon request. When a new methodology-driven report is requested, the customer must notify Bugcrowd to arrange for this style of testing to commence. Retesting can also be requested when vulnerabilities are remediated, in order to ensure a clean compliance report.

SECTION 2: PENETRATION TESTING METHODOLOGY

Testing Methodology

The methodology for performing a Max penetration test is split into four phases: reconnaissance, enumeration, exploitation, and documentation. When reviewing common industry penetration testing standards, such as NIST SP 800-115, Bugcrowd identified similarities in the workflow of industry standards and used these similarities to develop the methodology used in the penetration test. Schellman reviewed the defined testing methodology and confirmed that the phases adequately followed the guidance provided by NIST SP 800-115 on performing a phased information security assessment.

Each of the phases are executed in a cyclical manner allowing penetration testers to build upon findings and potentially uncover significant risks. The reconnaissance phase begins with the customer providing information regarding the scope of a Max penetration test. In this phase, customers will identify external URLs and IP addresses to be tested, provide access to internal environments, and provide information regarding the network architecture and segmentation controls. Additionally, the reconnaissance phase includes information gathering by the community of researchers selected for a Max penetration test.

The enumeration phase is where researchers identify attack vectors based on information gathered in the reconnaissance phase. Once a researcher has identified a vulnerability, they move to the exploitation phase and seek to verify the issue by creating a proof of concept to prove the existence of the vulnerability. The researcher completes the four phased process by reporting the vulnerability to Bugcrowd in the documentation phase. Bugcrowd personnel will then confirm the vulnerability is a legitimate issue that has not already been reported. If the vulnerability can be validated, and has not been reported in the past, Bugcrowd will triage, prioritize, and attach remediation advice to the vulnerability before providing the information to the customer. Customers can see all confirmed vulnerabilities in the vulnerability analytics dashboard that they access through their account in the Bugcrowd Platform.

Retesting

As part of its Penetration Test Max solution, Bugcrowd includes re-testing services to customers seeking to confirm that a vulnerability previously identified was successfully fixed. Bugcrowd employees conduct the test and update the vulnerability analytics dashboard, as well as the report. In an ongoing Penetration Test Max, there would be multiple instances in a given year where a confirmed vulnerability was remediated, and a Bugcrowd employee performed testing to confirm that remediation was effective.

Penetration Test Standard & Plus Methodology

Alignment with Industry Standards

Bugcrowd Penetration Test Standard and Plus utilize the same defined testing methodology as is leveraged for Penetration Test Max. Review of example Standard and Plus reports showed that the alignment with the aforementioned industry standards was consistent between the two solutions. Further review of the methodology, in conjunction with PCI DSS v3.2.1 requirements 6.6 and 11.3 / PCI DSS v4.0 requirements 6.4.1 and 11.4, can be found in section three of this white paper. Bugcrowd's methodology for conducting a Standard or Plus penetration test uses the same OWASP Testing Guide v4 and its web application security testing steps as the Penetration Test Max. Schellman observed example Standard and Plus reports and noted that each step was included in the testing practices.

Service Options

Bugcrowd's Penetration Test Standard service offering includes a standard penetration test for its customers with the ability to add on additional services such as expedited testing and retesting. Customers are responsible for ensuring that the scope of the Standard penetration test engagement is adequate to meet various regulatory and compliance requirements.

Bugcrowd's Penetration Test Plus service includes the same services as the Standard offering, with additional flexibility and customization options.

.

SECTION 2: PENETRATION TESTING METHODOLOGY

Testing Methodology

The methodology for performing the Penetration Test Standard and Plus are split into the same four phases as was enumerated for Penetration Test Max above. Schellman reviewed the defined testing methodology and confirmed that the phases adequately followed the guidance provided by NIST SP 800-115 on performing a phased information security assessment. The process for each of the four phases is the same as the Max process listed above. Similar to Max, customers can see all vulnerabilities as soon as they are submitted, in the vulnerability analytics dashboard which can be accessed through their account in the Bugcrowd Platform.

Retesting

Retesting to confirm a vulnerability has been successfully fixed is not included by default in Standard pen tests but can be added for a fee. However, retesting is included in the Plus package.

Penetration Test Basic Methodology

Alignment with Industry Standards

The Bugcrowd Penetration Test Basic service does not utilize the same defined testing methodology that is leveraged for the Max, Standard, and Plus penetration tests.

Testing Methodology

The methodology for performing a Penetration Test Basic Vulnerability Assessment consists of running an automated vulnerability scanning tool against the customer-defined targets to identify potential vulnerabilities. A human then reviews the results to remove false positives, potentially confirming that the issue exists when a payload exists.

Retesting

Retesting to confirm a vulnerability has been successfully fixed is not included by default in a Basic pen test but can be added for a fee.

SECTION 2: PENETRATION TESTING METHODOLOGY

Managed Bug Bounty Testing Methodology

Alignment with Industry Standards

Bugcrowd Managed Bug Bounty utilizes the same defined testing methodology, at a high level, as is leveraged for a Max penetration test. However, it does not utilize pre-defined security testing steps, leaving those up to the researchers performing the tests.

Testing Methodology

The high-level methodology for performing the Bug Bounty Test is split into the same four phases as was enumerated for Penetration Test Max above. Schellman reviewed the defined testing methodology and confirmed that the phases adequately followed the guidance provided by NIST SP 800-115 on performing a phased information security assessment. The process for each of the four phases is the same as the Penetration Test Max process listed above, with the exception that during the reconnaissance, enumeration, and exploitation phases, each individual tester determines what areas of the defined scope they want to test, and how much effort they put into the testing, rather than being required to follow prescribed testing steps. The documentation phase is the same as the Penetration Test Max one listed above. Similar to Max, customers can see all vulnerabilities as soon as they are submitted, in the vulnerability analytics dashboard which can be accessed through their account in the Bugcrowd Platform.

Retesting

Retesting to confirm a vulnerability has been successfully fixed is not included by default in Managed Bug Bounty but can be added for a fee.

SECTION 2: PENETRATION TESTING METHODOLOGY

Researcher & Penetration Tester Selection

During the course of the engagement, Bugcrowd provided information regarding the selection and categorization of security testers in their Crowdsourced community. Schellman did not perform testing or a review of this categorization process, but felt it was pertinent to include in this report. Only researchers and penetration testers that meet strict trust and skill requirements and have demonstrated success in the environment requiring testing are eligible to participate in Standard, Plus, and Max penetration tests and Managed Bug Bounty engagements. Depending on customer requirements, this level of vetting may include ID verification, background checks, and geolocation. Exceptionally talented and trusted testers are placed into the category of “Elite Crowd,” reserved for certain advanced engagements.

SKILL

A standard of high-impact submissions, averaging only high and critical submissions across a range of specific attack surface areas.

TRUST

Proven trust through ID verification and success working on private programs for top customers.

SECTION 3: COMPLIANCE REQUIREMENT NIST 800-53 REVISION 5

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
NIST 800-53 Rev5 CA-8. The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].	✓		✓	✓	✓	✓	Schellman reviewed the methodologies for Bugcrowd Penetration Test Standard, Plus, and Max solutions, and example reports for each and noted that testing performed by Bugcrowd supports this control.

ISO 27001 ANNEX A

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
ISO 27001 Annex A.12.6.1. Management of technical vulnerabilities. Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	✓	✓	✓	✓	✓	✓	Schellman reviewed the methodologies for Penetration Test Standard, Plus, and Max and example reports for each and noted that identification of vulnerabilities during Standard, Plus, and Max engagements supported the identification of vulnerabilities in a timely manner. Further, noted that customers were responsible for taking appropriate measures to address any risks identified during Standard, Plus, and Max engagements. Customers were solely responsible for the remediation of any vulnerabilities and then requesting retesting to prove the remediation is in place.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 6.6: For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:							
• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods – as follows:		✓	✓	✓	✓		Schellman observed Bugcrowd Penetration Test Standard, Plus, and Max methodologies along with sample penetration test reports for each type and noted that they met the requirements of a manual application vulnerability security assessment. Schellman observed Bugcrowd's Basic penetration test methodology along with sample Penetration Test Basic Vulnerability Assessment reports and noted that it met the requirements of an automated application vulnerability security assessment.
- At least annually.	✓	✓	✓	✓	✓	✓	A customer's use of Bugcrowd Penetration Test Standard, Plus, and Max to meet this requirement on an annual basis is contingent upon the following: • Customers are responsible for ensuring all applicable public-facing web applications are identified and communicated to Bugcrowd. • If a customer selects a timebound Max penetration test, the customer is responsible for ensuring the time frame identified is adequate to allow for complete testing of the public facing web application(s) in scope.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
- After any changes.	✓	✓	✓	✓	✓		Review of example Penetration Test Standard, Plus, and Max reports indicated that Bugcrowd's service offering directly support testing changes to public-facing web applications with the following caveats: • Only changes made during the contracted testing window would be tested. • If a timebound Max penetration test is selected by the customer, only changes that are made during the identified time frame will be tested. • Only applicable for a Plus penetration test if the change occurred just prior to the penetration test being performed. • A customer's use of a Basic penetration test to meet this requirement after any changes is contingent upon the following: • Customers are responsible for ensuring all applicable public-facing web applications are identified and communicated to Bugcrowd. All Penetration Test Basic engagements are unique. Customers are responsible for requesting that an engagement be "cloned" if desired, and scheduling the new engagement.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
- By an organization that specializes in application security.		✓	✓	✓	✓	✓	Schellman interviewed the Head of Operations at Bugcrowd and noted that researchers selected for Standard, Plus, and Max penetration tests and Managed Bug Bounty specialized in application security. Furthermore, Bugcrowd utilized a process for selecting researchers based on skill* observed during previous private and public bug bounty programs. * Additional information regarding researcher skill determination can be found in Section 2 of this white paper.
- That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment.		✓	✓	✓	✓		Schellman reviewed Bugcrowd's Standard, Plus, and Max penetration test methodologies and noted that application testing processes directly followed the OWASP testing Guide v4, which includes testing of all vulnerabilities identified in requirement 6.5.
- That all vulnerabilities are corrected.	✓						Bugcrowd customers are responsible for correcting all vulnerabilities identified. Bugcrowd provides guidance for remediating the vulnerabilities identified during the testing period, but it is the customer's responsibility to ensure all vulnerabilities are corrected.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
- That the application is re-evaluated after the corrections.	✓	✓	✓	✓	✓	✓	Customers are responsible for notifying Bugcrowd that a vulnerability has been corrected. Bugcrowd would then confirm that remediation activities conducted by the customer were effective. In the event that a customer has elected to use the timebound Penetration Test Max service, the customer is responsible for ensuring that the time frame of the test allows Bugcrowd the ability to conduct retesting. For a Standard penetration test, in order for the customer to have their remediation efforts confirmed, they would have to purchase the retesting add-on from Bugcrowd as it is not included as part of the Penetration Test Standard package. For a Plus penetration test, one retest is included; the customer would have to purchase additional retests if needed. For a Basic penetration test, retests are not available. The customer would have to purchase an add-on to their existing Basic package with the appropriate scope.
• Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	✓						Not applicable. Customers using Bugcrowd Penetration Test Standard, Plus, and Max services do not need to implement an automated technical solution to meet PCI requirement 6.6.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
11.3: Implement a methodology for penetration testing that includes the following:							
• Is based on industry-accepted penetration testing approaches (for example, NIST SP 800-115).	✓		✓	✓	✓	✓	Schellman reviewed Bugcrowd's Standard, Plus, and Max penetration test methodologies and noted that they aligned with NIST SP 800-115 and the OWASP Testing Guide v4. As recommended by NIST SP 800-115, the methodology provided to Schellman was repeatable, included the objective of the testing and contained processes for defining and categorizing vulnerabilities. Bugcrowd's Standard, Plus, and Max penetration test methodologies also included each step defined in the OWASP testing Guide v4. Schellman reviewed Bugcrowd's Managed Bug Bounty Testing methodology and noted that it aligned at a high level with NIST SP 800-115 and the OWASP Testing Guide v4. As recommended by NIST SP 800-115, the methodology provided to Schellman was repeatable, included the objective of the testing and contained processes for defining and categorizing vulnerabilities. However, security testing steps used by individual testers are not included in the methodology. Customers using the Managed Bug Bounty service are responsible for ensuring adequate testing coverage.
• Includes coverage for the entire CDE perimeter and critical systems.	✓		✓	✓	✓		Bugcrowd's customers are responsible for defining the scope of the environment to be tested. Once the customer has confirmed the scope of the assessment, they are responsible for providing this information to Bugcrowd and ensuring it includes the entire perimeter of the environment and all critical systems. Regarding internal penetration testing, Bugcrowd Penetration Test Plus and Max solutions can only cover systems and environments for which the customer identifies and provides access. Further, the Standard service tier does not include internal testing.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• Includes testing from both inside and outside the network.	✓			✓	✓		Bugcrowd Penetration Test Plus and Max solutions have the capacity to test various aspects of a customer's environment from both inside and outside of the network. It is the customer's responsibility to ensure Bugcrowd's testers have access to systems inside the network if the customer desires internal testing to be completed. The customer is also responsible for granting access to internal network segments. Regarding internal penetration testing, Bugcrowd's Plus and Max solutions can only cover systems and environments for which the customer identifies and provides access. Further, the Standard service tier does not include internal testing.
• Includes testing to validate any segmentation and scope-reduction controls.	✓			✓	✓		Customers are responsible for defining and determining the appropriateness of segmentation controls in their environments. Bugcrowd Penetration Plus and Max solutions have the capacity to assist in meeting PCI requirements for segmentation testing as long as the customer does the following: • Customers must request segmentation testing. • Customers are responsible for defining segmentation controls and interpreting the results of the segmentation test to determine if segmentation controls implemented by the customer are operational and effective. • Customers must include all segmentation controls/methods in the information provided to Bugcrowd in order to ensure all controls/ methods are tested.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.			✓	✓	✓		Schellman observed Bugcrowd Standard, Plus, and Max penetration test methodologies and noted that application testing processes directly followed the OWASP testing Guide v4, which includes testing of all vulnerabilities identified in requirement 6.5.
• Defines network-layer penetration tests to include components that support network functions as well as operating systems.	✓						Observation of example penetration tests conducted under Standard, Plus, and Max penetration test methodologies indicate that customers are responsible for defining network-layer penetration tests. Through interviews with the Head of Operations at Bugcrowd, Schellman noted that Bugcrowd had the capacity to conduct network-layer penetration testing, but customers were responsible for defining and identifying components that support network functions, and customers must request network-layer penetration testing as part of their Standard, Plus, or Max penetration test engagements. Additionally, the purchase of an add-on may be required.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.	✓						As part of Bugcrowd's broader vulnerability management service offerings, Bugcrowd offers customers access to a platform that contains a vulnerability analytics dashboard. Customers of the Bugcrowd Penetration Plus and Max solutions (and Managed Bug Bounty if purchased for a term of at least 12 months) have access to these services for viewing and progressing vulnerabilities through the security development lifecycle. Schellman observed an example of the vulnerability analytics dashboard and noted that it was designed to retain vulnerability information for the duration of a customer's relationship with Bugcrowd. Customers are responsible for retaining the formal penetration test reports and findings delivered to them at the end of all penetration test engagements. Customers are also responsible for retaining all vulnerabilities identified prior to the start of services from Bugcrowd. Further, customers are responsible for maintaining a vulnerability management policy in conjunction with PCI requirement 6.1, and informing Bugcrowd of any threats and vulnerabilities experienced in the last 12 months for review and consideration for inclusion in testing.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• Specifies retention of penetration testing results and remediation activities results.	✓		✓	✓	✓	✓	Schellman observed Bugcrowd's penetration testing methodology and noted that retention of testing results would occur for the duration of the contracted relationship between Bugcrowd and their customers. Customers have a shared responsibility to maintain formal testing results as part of their applicable data retention and vulnerability management policies. Customers electing to use Bugcrowd Penetration Test Standard, Plus, and timebound Max solutions, as well as Managed Bug Bounty, are responsible for retaining all testing results after the defined period has concluded with Bugcrowd. Although Bugcrowd retains information regarding the vulnerabilities, the customer is ultimately responsible for retaining formal reports for the purposes of meeting regulatory requirements to include the PCI-DSS.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
11.3.1: Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).							
PCI 11.3.1.a Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows: • Per the defined methodology. • At least annually. • After any significant changes to the environment.	✓		✓	✓	✓		Schellman observed program details and example penetration testing reports under Bugcrowd Penetration Test Standard, Plus, and Max solutions and noted the following: • Customers are responsible for defining the scope of external penetration tests. • Observation of the example penetration test reports shared with Schellman indicated the defined methodology was followed. • Use of a Max penetration test provides direct support for conducting external penetration testing on an annual basis with a formal report being delivered at an agreed upon date. Additional testing periods and subsequent reports can be purchased on top of any Max penetration test engagement. Bugcrowd Penetration Test Max allows for ongoing testing of customer environments. Depending on the significance of a change, customers will likely need to notify Bugcrowd to ensure the methodology includes checks for additional security issues introduced by the change to the customers environment.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• **PCI 11.3.1.b** Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).			✓	✓	✓	✓	Schellman interviewed the Head of Operations at Bugcrowd and noted that penetration testers selected for Standard, Plus, and Max penetration tests were qualified to conduct external penetration tests. Furthermore, Bugcrowd utilized a process for selecting testers based on skill*. Finally, Bugcrowd's Crowdsourced researchers were neither involved in remediation activities nor were they involved in retesting thus indicating organizational independence. *Additional information regarding researcher skill determination can be found in section 2 of this white paper.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.3.2 Perform ***internal*** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).							
PCI 11.3.2.a Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows. • Per the defined methodology. • At least annually. • After any significant changes to the environment.	✓			✓	✓		Schellman observed program details and example penetration test reports for the Bugcrowd Penetration Test Plus and Max service offerings* and noted the following: • Customers are responsible for defining the scope of internal penetration tests. • Observation of the example penetration tests shared with Schellman indicated the defined methodology was followed. • Use of the continuous testing service option provides direct support for conducting internal penetration testing on an annual basis with a formal report being delivered at an agreed upon date. • The continuous testing service option for Penetration Test Max allows for ongoing testing of customer environments after incremental changes to the environment. Depending on the nature of a change, customers will likely need to notify Bugcrowd to ensure testing includes checks for additional security issues introduced by the change to the customers environment. • Customers choosing to conduct a timebound Max penetration test will need to ensure the duration of time is adequate to address any significant changes and that a timebound penetration test is conducted at least annually. * The customer would have to select an additional option to include the internal network and segmentation in their penetration testing and report. The Standard service tier does not include internal testing. Customers would need to use the Plus or Max tiers to include internal targets.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.3.2.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).				✓	✓		Schellman interviewed the Head of Security at Bugcrowd and noted that penetration testers selected for Bugcrowd Penetration Test Plus and Max were qualified to conduct internal penetration tests. Further, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's penetration testers were not involved in remediation activities, nor were they involved in retesting thus indicating organizational independence.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.3.3: Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.							
PCI 11.3.3 Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.	✓		✓	✓	✓	✓	Because customers are responsible for all remediation activities, customers also share the responsibility for the re-evaluation of all corrected vulnerabilities. Customers are responsible for notifying Bugcrowd that an exploitable vulnerability previously identified by Bugcrowd has been remediated. Bugcrowd will then use Bugcrowd employees, unless customers want the retesting to be done by researchers, to confirm that remediation activities conducted by the customer were effective. In the event that a customer has elected to use the timebound service option for a Max penetration test, the customer is responsible for ensuring that the period identified allows Bugcrowd the ability to conduct retesting. For Bugcrowd Penetration Test Standard, in order for the customer to have their remediation efforts confirmed, they would have to purchase the retesting add-on from Bugcrowd as it is not included as part of the Standard package. For a Plus penetration test, one retest is included; the customer would have to purchase additional retests if needed. For a Basic penetration test, retests are not available. The customer would have to purchase a new Basic penetration test with the appropriate scope.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.3.4: If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.							
PCI 11.3.4.a Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	✓			✓	✓		Customers are responsible for defining and determining the appropriateness of segmentation controls in their environments. Bugcrowd Penetration Test Plus and Max solutions have the capacity to assist in meeting PCI requirements for segmentation testing as long as the customer does the following: • Customers must request segmentation testing. • Customers are responsible for defining segmentation controls and interpreting the results of the segmentation test to determine if segmentation controls are operational and effective. • Customers must include all segmentation controls/methods in the information provided to Bugcrowd in order to ensure all controls/methods are tested.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.3.4.b Examine the results from the most recent penetration test to verify that: • Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	✓			✓	✓		Customers are responsible for defining and determining the appropriateness of segmentation controls in their environments. Bugcrowd Penetration Test Plus and Max solutions have the capacity to assist in meeting PCI requirements for segmentation testing as long as the customer does the following: • Customers must request segmentation testing as a part of the annual penetration test report. • Customers must request a segmentation only penetration test at the midpoint between the two annual reports (six-month mark). • Customers are responsible for defining segmentation controls and interpreting the results of the segmentation test to determine if segmentation controls are operational and effective. • Customers must include all segmentation controls/methods in the information provided to Bugcrowd in order to ensure all controls/ methods are tested. • Customers must inform Bugcrowd of and segmentation changes to controls/methods and the requirement to perform a penetration test to prove the change did not have a negative security impact. Note: For a Plus penetration test ,a separate penetration test will be required for the semi-annual segmentation test. For customers choosing a timebound Max penetration test, a separate penetration test may be required depending on the time period for the penetration test.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.3.4.c Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	✓			✓	✓		Schellman interviewed the Head of Security at Bugcrowd and noted that penetration testers selected for Bugcrowd Penetration Test Plus and Max were qualified to conduct internal penetration tests. Further, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's penetration testers were not involved in remediation activities, nor were they involved in retesting thus indicating organizational independence. Customers are responsible for ensuring the organizational independence of individuals that review the segmentation test findings to determine if segmentation controls implemented by the customer are operational and effective.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.3.4.1 *Additional requirement for service providers only:* If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.							
PCI 11.3.4.1.a Examine the results from the most recent penetration test to verify that: • Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/ methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	✓			✓	✓		Bugcrowd Penetration Test Plus and Max solutions have the capacity to assist in meeting PCI requirements for segmentation testing as long as the customer does the following: • Customers must request segmentation testing to be conducted every six months. • Customers are responsible for defining segmentation controls and interpreting the results of the segmentation test to determine if segmentation controls implemented are operational and effective. • Customers must include all segmentation controls/method in the information provided to Bugcrowd to ensure all controls/methods are tested.

SECTION 3: COVERAGE PCI DSS V3.2.1

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.3.4.1.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	✓			✓	✓		Schellman interviewed the Head of Security at Bugcrowd and noted that penetration testers selected for Bugcrowd Penetration Test Plus and Max were qualified to conduct internal penetration tests. Further, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's penetration testers were not involved in remediation activities, nor were they involved in retesting thus indicating organizational independence. Customers are responsible for ensuring the organizational independence of individuals that review the segmentation test findings to determine if segmentation controls implemented by the customer are operational and effective.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: **Applicable if a PCI DSS assessment is finished prior to 31 March 2025 only:**							
• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:		✓	✓	✓	✓		Schellman observed Bugcrowd Penetration Test Standard, Plus, and Max methodologies along with sample penetration test reports for each type and noted that they meet the requirements of a manual application vulnerability security assessment. Schellman observed Bugcrowd's Basic penetration test methodology along with sample Penetration Test Basic Vulnerability Assessment reports and noted that they meet the requirements of an automated application vulnerability security assessment. Note: After 31 March 2025, this requirement will no longer be applicable. Customers are responsible for complying with requirement 6.4.2 after that time.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
– At least once every 12 months and after significant changes.	✓	✓	✓	✓	✓	✓	A customer's use of a Basic, Standard, Plus, or Max penetration test to meet this requirement on an annual basis is contingent upon the following: • Customers are responsible for ensuring all applicable public-facing web applications are identified and communicated to Bugcrowd. If a customer selects a timebound Max penetration test, the customer is responsible for ensuring the time frame identified is adequate to allow for complete testing of the public facing web application(s) in scope. **With regard to changes:** Review of example Bugcrowd Penetration Test Standard, Plus, and Max reports indicated that Bugcrowd's service offering directly support testing changes to public-facing web applications with the following caveats: • Only changes made during the contracted testing window would be tested. • If a timebound Max penetration test is selected by the customer, only changes that are made during the identified time frame will be tested. • Only applicable for a Plus penetration test if the change occurred just prior to the penetration test being performed. A customer's use of a Basic penetration test to meet this requirement after any changes is contingent upon the following: • Customers are responsible for ensuring all applicable public-facing web applications are identified and communicated to Bugcrowd. • Each Penetration Test Basic engagement is unique. Customers are responsible for requesting that an engagement be "cloned" if desired, and scheduling the new engagement.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
– By an entity that specializes in application security.		✓	✓	✓	✓	✓	Schellman interviewed the Head of Operations at Bugcrowd and noted that researchers selected for Bugcrowd Penetration Test Standard, Plus and Max and Managed Bug Bounty specialized in application security. Furthermore, Bugcrowd utilized a process for selecting researchers based on skill* observed during previous private and public bug bounty programs. * Additional information regarding researcher skill determination can be found in Section 2 of this white paper.
– Including, at a minimum, all common software attacks in Requirement 6.2.4.		✓	✓	✓	✓		Schellman reviewed Bugcrowd's Standard, Plus, and Max penetration test methodologies and noted that application testing processes directly followed the OWASP Testing Guide v4, which includes testing of common software attacks in Requirement 6.2.4.
– All vulnerabilities are ranked in accordance with requirement 6.3.1.	✓		✓	✓	✓	✓	Schellman reviewed Bugcrowd's Standard, Plus and Max penetration test and Managed Bug Bounty methodologies and noted that Bugcrowd risk ranks vulnerabilities in accordance with a standard vulnerability rating taxonomy based on their experience over the last ten years. Customers are responsible for risk ranking vulnerabilities in accordance with requirement 6.3.1.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
– All vulnerabilities are corrected.	✓						Bugcrowd customers are responsible for correcting all vulnerabilities identified. Bugcrowd provides guidance for remediating the vulnerabilities identified during the testing period, but it is the customer's responsibility to ensure all vulnerabilities are corrected.
– The application is re-evaluated after the corrections.	✓	✓	✓	✓	✓	✓	Customers are responsible for notifying Bugcrowd that a vulnerability has been corrected. Bugcrowd will then confirm that remediation activities conducted by the customer were effective. In the event that a customer has elected to use the timebound Penetration Test Max service, the customer is responsible for ensuring that the time frame of the test allows Bugcrowd the ability to conduct retesting. For a Standard penetration test, in order for the customer to have their remediation efforts confirmed, they would have to purchase the retesting add-on from Bugcrowd as it is not included as part of the Standard package. For a Plus penetration test, one retest is included; the customer would have to purchase additional retests if needed. For a Basic penetration test, retests are not available. The customer would have to purchase a new Basic penetration test with the appropriate scope.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
Beginning 31 March 2025: **PCI 6.4.2** For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated. **Note:** This requirement is a **best practice** until **31 March 2025**, after which it will be required and must be fully considered during a PCI DSS assessment. This new requirement will replace Requirement 6.4.1 once its effective date is reached.	✓						As of 31 March 2025, PCI DSS requirement 6.4.1 will be replaced by PCI DSS Requirement 6.4.2. As of that time, all public-facing web applications must have an automated technical solution deployed that continually detects and prevents web-based attacks as described in this requirement. Customers are responsible for deploying an automated technical solution that complies with PCI DSS 6.4.2 no later than 31 March 2025.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity and includes:							
• Industry-accepted penetration testing approaches.	✓		✓	✓	✓	✓	Schellman reviewed Bugcrowd's Standard, Plus, and Max penetration test methodologies and noted that they aligned with NIST SP 800-115 and the OWASP Testing Guide v4. As recommended by NIST SP 800-115, the methodology provided to Schellman was repeatable, included the objective of the testing and contained processes for defining and categorizing vulnerabilities. Bugcrowd's Standard, Plus, and Max penetration test methodologies also included each step defined in the OWASP testing Guide v4. Schellman reviewed Bugcrowd's Managed Bug Bounty testing methodology and noted that it is aligned at a high level with NIST SP 800-115 and the OWASP Testing Guide v4. As recommended by NIST SP 800-115, the methodology provided to Schellman was repeatable, included the objective of the testing and contained processes for defining and categorizing vulnerabilities. However, security testing steps used by individual testers are not included in the methodology. Customers using the Managed Bug Bounty service are responsible for ensuring adequate testing coverage.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• Coverage for the entire CDE perimeter and critical systems.	✓		✓	✓	✓		Bugcrowd's customers are responsible for defining the scope of the environment to be tested. Once the customer has confirmed the scope of the assessment, they are responsible for providing this information to Bugcrowd and ensuring it includes the entire perimeter of the environment and all critical systems. Regarding internal penetration testing, Bugcrowd Penetration Test Plus and Max solutions can only cover systems and environments for which the customer identifies and provides access. Further, the Standard service tier does not include internal testing. Customers would need to purchase an internal testing add-on to ensure internal testing is included.
• Testing from both inside and outside the network.	✓			✓	✓		Bugcrowd Penetration Test Standard, Plus, and Max solutions have the capacity to test various aspects of a customer's environment from both inside and outside of the network. It is the customer's responsibility to ensure Bugcrowd's testers have access to systems inside the network if the customer desires internal testing to be completed. The customer is also responsible for granting access to internal network segments. Regarding internal penetration testing, Bugcrowd's Plus and Max penetration test solutions can only cover systems and environments for which the customer identifies and provides access. Further, the Standard service tier does not include internal testing.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4.			✓	✓	✓		Schellman observed Bugcrowd's Standard, Plus, and Max penetration test methodologies and noted that application testing processes directly followed the OWASP testing Guide v4, which includes testing of all vulnerabilities identified in requirement.
• Network-layer penetration tests that encompass all components that support network functions as well as operating systems.	✓						Observation of example penetration tests conducted under Standard, Plus, and Max penetration test methodologies indicate that customers are responsible for defining network-layer penetration tests. Through interviews with the Head of Operations at Bugcrowd, Schellman noted that Bugcrowd had the capacity to conduct network-layer penetration testing, but customers were responsible for defining and identifying components that support network functions, and customers must request network-layer penetration testing as part of their Standard, Plus or Max engagements. Additionally, the purchase of an add-on may be required.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• Review and consideration of threats and vulnerabilities experienced in the last 12 months.	✓						As part of Bugcrowd's broader vulnerability management service offerings, Bugcrowd offers customers access to a platform that contains a vulnerability analytics dashboard. Customers of the Bugcrowd Penetration Test Plus and Max solutions have access to these services for viewing and progressing vulnerabilities through the security development lifecycle. Schellman observed an example of the vulnerability analytics dashboard and noted that it was designed to retain vulnerability information for the duration of a customer's relationship with Bugcrowd. Customers are responsible for retaining the formal penetration test reports and findings delivered to them at the end of all Penetration Test engagements. Customers are also responsible for retaining all vulnerabilities identified prior to the start of services from Bugcrowd. Further, customers are responsible for maintaining a vulnerability management policy in conjunction with PCI requirement 6.3.1
• Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing.	✓						Customers are responsible for assessing and addressing the risk posed by vulnerabilities and weaknesses in their environment.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• Retention of penetration testing results and remediation activities results for at least 12 months.	✓		✓	✓	✓	✓	Schellman observed Bugcrowd's penetration testing methodology and noted that retention of testing results would occur for the duration of the contracted relationship between Bugcrowd and their customers. Customers have a shared responsibility to maintain formal testing results as part of their applicable data retention and vulnerability management policies. Customers electing to use Bugcrowd Penetration Test Standard, Plus, and timebound Max solutions are responsible for retaining all testing results after the defined period has concluded with Bugcrowd. Although Bugcrowd retains information regarding the vulnerabilities, the customer is ultimately responsible for retaining formal reports for the purposes of meeting regulatory requirements to include the PCI-DSS.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.4.2 Internal penetration testing is performed:							
• Per the entity's defined methodology. • At least once every 12 months. • After any significant infrastructure or application upgrade or change.	✓			✓	✓		Schellman observed program details and example penetration test reports for the Bugcrowd Penetration Test Plus and Max service offerings* and noted the following: • Customers are responsible for defining the scope of internal penetration tests. • Observation of the example penetration tests shared with Schellman indicated the defined methodology was followed. • Use of the continuous testing service option provides direct support for conducting internal penetration testing on an annual basis with a formal report being delivered at an agreed upon date. • The continuous testing service option for a Max penetration test allows for ongoing testing of customer environments after incremental changes to the environment. Depending on the nature of a change, customers will likely need to notify Bugcrowd to ensure testing includes checks for additional security issues introduced by the change to the customers environment. • Customers choosing to conduct a timebound Max penetration test will need to ensure the duration of time is adequate to address any significant changes and that a Standard or Plus or timebound penetration test is conducted at least annually. * The customer would have to select an additional option to include the internal network and segmentation in their penetration testing and report. The Standard service tier does not include internal testing. Customers would need to purchase the Plus or Max tier to include internal targets.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• By a qualified internal resource or qualified external third-party.				✓	✓		Schellman interviewed the Head of Security at Bugcrowd and noted that penetration testers selected for Bugcrowd Penetration Test Plus and Max were qualified to conduct internal penetration tests. Further, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's penetration testers were not involved in remediation activities, nor were they involved in retesting thus indicating organizational independence.
• Organizational independence of the tester exists (not required to be a QSA or ASV).				✓	✓		Schellman interviewed the Head of Security at Bugcrowd and noted that penetration testers selected for Plus and Max penetration tests were qualified to conduct internal penetration tests. Further, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's penetration testers were not involved in remediation activities, nor were they involved in retesting thus indicating organizational independence.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.4.3 External penetration testing is performed:							
• Per the entity’s defined methodology. • At least once every 12 months. • After any significant infrastructure or application upgrade or change.	✓		✓	✓	✓		Schellman observed program details and example penetration testing reports under Bugcrowd Penetration Test Standard, Plus nd Max solutions and noted the following: • Customers are responsible for defining the scope of external penetration tests. • Observation of the example penetration test reports shared with Schellman indicated the defined methodology was followed. Use of Max penetration test provides direct support for conducting external penetration testing on an annual basis with a formal report being delivered at an agreed upon date. Additional testing periods and subsequent reports can be purchased on top of any Max penetration test engagement. Bugcrowd Penetration Test Max allows for ongoing testing of customer environments. Depending on the significance of a change, customers will likely need to notify Bugcrowd to ensure the methodology includes checks for additional security issues introduced by the change to the customers environment.
• By a qualified internal resource or qualified external third-party. • Organizational independence of the tester exists (not required to be a QSA or ASV).			✓	✓	✓	✓	Schellman interviewed the Head of Operations at Bugcrowd and noted that penetration testers selected for Standard, Plus, and Max penetration tests were qualified to conduct external penetration tests. Furthermore, Bugcrowd utilized a process for selecting testers based on skill*. Finally, Bugcrowd’s Crowdsourced researchers were neither involved in remediation activities nor were they involved in retesting thus indicating organizational independence.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows:							
• In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1.	✓						Bugcrowd customers are responsible for correcting all vulnerabilities identified. Bugcrowd provides guidance for remediating the vulnerabilities identified during the testing period, but it is the customer's responsibility to ensure all vulnerabilities are corrected.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• Penetration testing is repeated to verify the corrections.	✓		✓	✓	✓	✓	Because customers are responsible for all remediation activities, customers also share the responsibility for the re-evaluation of all corrected vulnerabilities. Customers are responsible for notifying Bugcrowd that an exploitable vulnerability previously identified by Bugcrowd has been remediated. Bugcrowd will then use Bugcrowd employees, not the pool of Crowdsourced researchers, to confirm that remediation activities conducted by the customer were effective. In the event that a customer has elected to use the timebound service option for a Max penetration test, the customer is responsible for ensuring that the period identified allows Bugcrowd the ability to conduct retesting. For a Standard penetration test, in order for the customer to have their remediation efforts confirmed, they would have to purchase the retesting add-on from Bugcrowd as it is not included as part of the Standard package. For a Plus penetration test, one retest is included; the customer would have to purchase additional retests if needed. For a Basic penetration test, retests are not available. The customer would have to purchase a new Basic penetration test with the appropriate scope.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:							
• At least once every 12 months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).	✓			✓	✓		Customers are responsible for defining and determining the appropriateness of segmentation controls in their environments. Bugcrowd Penetration Test Plus and Max solutions have the capacity to assist in meeting PCI requirements for segmentation testing as long as the customer does the following: • Customers must request segmentation testing. • Customers are responsible for defining segmentation controls and interpreting the results of the segmentation test to determine if segmentation controls are operational and effective. Customers must include all segmentation controls/methods in the information provided to Bugcrowd in order to ensure all controls/ methods are tested.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	✓			✓	✓		Schellman interviewed the Head of Security at Bugcrowd and noted that penetration testers selected for Standard, Plus, and Max penetration tests were qualified to conduct internal penetration tests. Further, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's penetration testers were not involved in remediation activities, nor were they involved in retesting thus indicating organizational independence. Customers are responsible for ensuring the organizational independence of individuals that review the segmentation test findings to determine if segmentation controls implemented by the customer are operational and effective.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
PCI 11.4.6 ***Additional requirement for service providers only:*** If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:							
• At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).	✓			✓	✓		Bugcrowd Penetration Test Plus and Max solutions have the capacity to assist in meeting PCI requirements for segmentation testing as long as the customer does the following: • Customers must request segmentation testing to be conducted every six months. • Customers are responsible for defining segmentation controls and interpreting the results of the segmentation test to determine if segmentation controls implemented are operational and effective. Customers must include all segmentation controls/method in the information provided to Bugcrowd to ensure all controls/methods are tested.

SECTION 4: COMPLIANCE REQUIREMENT COVERAGE PCI DSS V4.0

Compliance Requirements	Responsibility						Assessor Findings
	Cust	PTB	PTS	PTP	PTM	MBB	
• Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	✓			✓	✓	✓	Schellman interviewed the Head of Security at Bugcrowd and noted that penetration testers selected for Standard, Plus, and Max penetration tests were qualified to conduct internal penetration tests. Further, Bugcrowd utilized a process for selecting researchers based on skill. Additional information regarding researcher skill determination can be found in section 2 of this white paper. Finally, Bugcrowd's penetration testers were not involved in remediation activities, nor were they involved in retesting thus indicating organizational independence. Customers are responsible for ensuring the organizational independence of individuals that review the segmentation test findings to determine if segmentation controls implemented by the customer are operational and effective.
• **PCI 11.4.7** ***Additional requirement for multi-tenant service providers only:*** Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4. • **Note:** This requirement is a **best practice** until **31 March 2025**, after which it will be required and must be fully considered during a PCI DSS assessment.	✓						Customers are responsible for implementing this requirement.

www.schellman.com

schellman