



BPO Convergence

Monthly IT Evaluation & Testing Report

Sat, 01 Feb 2025



All information contained in this document is proprietary of BPO Convergence Pvt Ltd Company. The content, terms, and details of this report, in whole or in part, are strictly confidential and contain intellectual property, information, and ideas owned by BPO Convergence Pvt Ltd. This report or any of its contents may only be used for its internal use and may not be disclosed to any third party without written consent from BPO Convergence Pvt Ltd.

The information in this documentation is subject to change without notice and should not be construed as a commitment by BPO Convergence Pvt Ltd. BPO Convergence Pvt Ltd. makes no representations or warranties, express or implied, with respect to the documentation and shall not be liable for any damages, including any indirect, incidental, consequential damages (such as loss of profit, loss of use of assets, loss of business opportunity, loss of data or claims for or on behalf of user's customers), that may be suffered by the user.

© 2025 – BPO Convergence Pvt. Ltd. India

www.bpoconvergence.com

CONTENTS

ENGAGEMENT DETAILS:	3
Limitations on Disclosure and Use of This Report	5
Confidentiality	5
SUMMARY:	6
Vulnerability Summary	7
Executive Summary	7
METHODOLOGY:	9
Assessment Type	9
Risk Assessment Methodology	9
FINDINGS TABLE:	11
Services by Host & by Open Port:	11
FINDING DETAILS:	12
Minimal Priority Findings:	12
1 – Sensitive Information Disclosure	12

ENGAGEMENT DETAILS:

ASSESSMENT SUMMARY

Engagement Timeframe	Swiggy Process
Assessment ID	Swiggy OMT/CHAT
Application Type	Internal Network
Authors	Amar Singh
Penetration Tester	Chanchal Kanjilal
Report Version	4.5
Last Update	01/02/2025

ASSESSMENT SCOPE SUMMARY

The scope of this assessment was limited to components and interfaces specific to Company External Network.

In scope Network Name	Swiggy Network
In Scope	Antivirus Patch, Domain Status, Policy Update & Others
Environment	Production
In scope User roles	N/A
Out of Scope	Anything Excluding the In Scope IP.

Limitations on Disclosure and Use of This Report

This report contains information concerning potential vulnerabilities of in-scope network and methods of exploiting them. Organization recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein.

Security assessment is an uncertain process, based upon past experiences, currently available information, and known threats. It should be understood that all information systems, which by their nature are dependent on human beings, are vulnerable to some degree.

Therefore, while Organization considers the major security vulnerabilities of the analysed network to have been identified, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures.

In addition, the analysis set forth herein is based on the technologies and known threats as of the date of this report. As technologies and risks change over time, the vulnerabilities associated with the operation of the target external network described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities will also change.

This report may recommend that the target network use certain software or hardware products manufactured or maintained by other vendors.

This report was prepared by Internal IT team for the exclusive use and benefit of target systems and is deemed proprietary information.

Confidentiality

This document contains information that is confidential and proprietary, which shall not be disclosed outside Authorize person/company, transmitted, or duplicated, used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without explicit written permission of network owner is prohibited.

SUMMARY:

This report presents the results of the Security Testing of Scope in network. The purpose of this assessment is to identify network and related network-level security issues that could affect the target network – remediate it before the network is fully launched to its users.

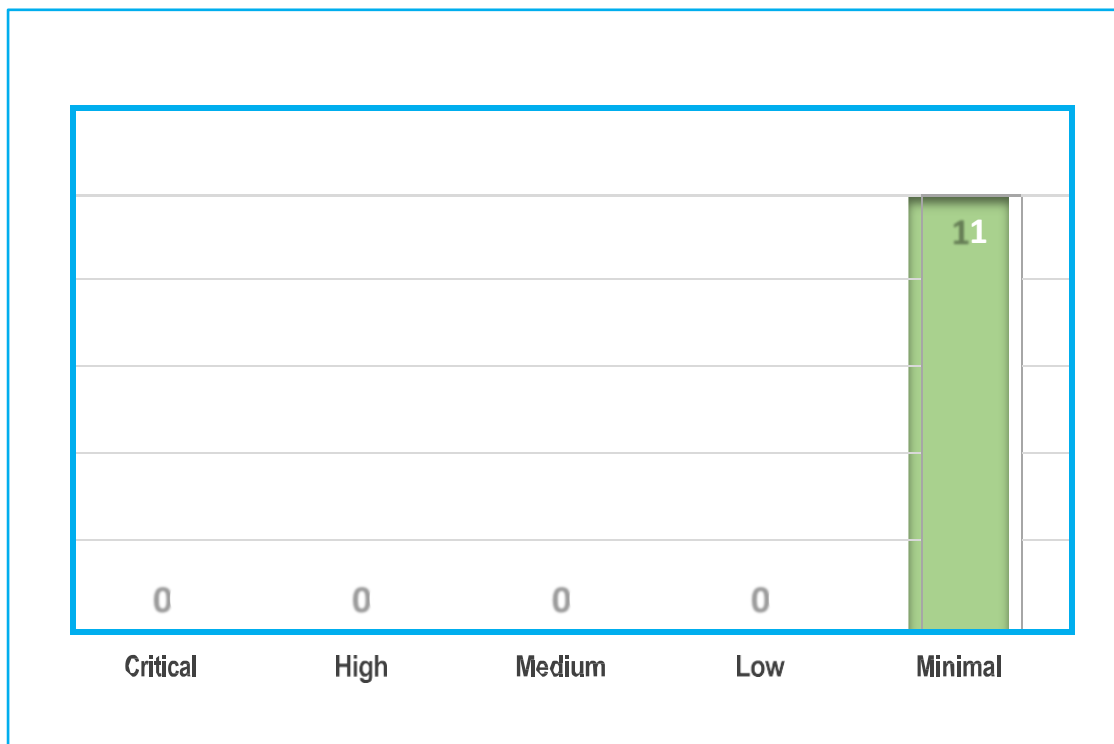
To evaluate the security of the network and network, IT team attempted to perform unauthorized transactions, obtain confidential information, and determine the overall security of the network by performing a wide variety of vulnerability checks.

The testing also included the servers and technologies associated with the organization and network. This result is intended to be an assessment of the targeted network and any asset that fall within the scope of this project.

Furthermore, the findings in this report reflect the conditions found during the testing, and do not necessarily reflect current conditions. The objective of the analysis is to simulate an attack to assess and discover weak links and provide recommendations and guidelines to vulnerable entities discovered. Every issue includes an overview, issues found and security guidelines, which, if followed correctly, will ensure the confidentiality and integrity of the systems and network.

Vulnerability Summary

The following Number of vulnerabilities were found at each risk level. It is essential to know that total vulnerabilities are not a factor in determining the risk level. The risk level is depending upon the severity of the vulnerabilities found.



Executive Summary

BPO Convergence Pvt Ltd. conducted Internal Test for “Noida”. This test was performed to assess target systems defensive posture and provide security assistance through proactively identifying vulnerabilities, validating their severity, and providing remediation steps.

Our security assessment revealed ‘1’ vulnerabilities (‘1’ Minimal Risks) in the target Network.

Grading Criteria's:

Grade	Level	Criteria Description
A	Excellent	The security exceeds "Industry Best Practice" standards. The overall posture was found to be excellent with only a few low-risk findings identified.
B	Good	The security meets with accepted standards for "Industry Best Practice." The overall posture was found to be strong with only a handful of medium- and low- risk shortcomings identified.
C	Fair	Current solutions protect some areas of the enterprise from security issues. Moderate changes are required to elevate the discussed areas to "Industry Best Practice" standards.
D	Unsatisfactory	Significant security deficiencies exist. Immediate attention should be given to the discussed issues to address exposures identified. Major changes are required to elevate to "Industry Best Practice" standards.
E	Inadequate	Serious security deficiencies exist. Shortcomings were identified throughout most or even all of the security controls examined. Improving security will require a major allocation of resources.

METHODOLOGY:

Assessment Type

IT team was engaged to perform a time-boxed manual security assessment against the target network. This assessment involved a deep automated scan using automated scanning tools to discover common vulnerabilities, as well as manual testing. Manual testing includes validation of all issue types covered under the automated scan as well as checks for problems not typically found by automated scanners.

Risk Assessment Methodology

The severity assigned to each vulnerability was calculated using the NIST 800-30 Revision 1 standard. This standard determines the risk posed by application based on the likelihood an attacker exploits the vulnerability and the impact that it would have on the business.

Likelihood

The difficulty of exploiting the security vulnerability described includes required skill level and the amount of access necessary to visit the element susceptible to the vulnerability. The difficulty is rated with the following values:

Critical: An attacker is almost certain to initiate the threat event.

High: An untrained user could exploit vulnerability, or the vulnerability is obvious and easily accessible.

Medium: The vulnerability requires some hacking knowledge or access is restricted in some way.

Low: Exploiting vulnerability requires application access, significant time, resources or a specialized skillset.

Minimal: Adversaries are highly unlikely to leverage vulnerability.

Impact

The impact the vulnerability would have on the organization if it were successfully exploited is rated as follows:

Critical: The issue causes multiple severe or catastrophic effects on organizational operations, organizational assets or other organizations.

High: Exploitation produces severe degradation in mission capability to the point that the organization is not able to perform primary functions or results in damage to organizational assets.

Medium: Threat events trigger degradation in mission capability to an extent the application is able to perform its primary functions, but their effectiveness is reduced and there may be damage to organizational assets.

Low: Successful exploitation has limited degradation in mission capability; the organization is able to perform its primary functions, but their effectiveness is noticeably reduced and may result in minor damage to organizational assets.

Minimal: The threat could have a negligible adverse effect on organizational operations or organizational assets.

Severity

The vulnerability severity is determined using the likelihood and impact weights in the following table:

		Impact				
		<i>Minimal</i>	<i>Low</i>	<i>Medium</i>	<i>High</i>	<i>Critical</i>
Likelihood	<i>Critical</i>	Minimal	Low	Medium	High	Critical
	<i>High</i>	Minimal	Low	Medium	High	Critical
	<i>Medium</i>	Minimal	Low	Medium	Medium	High
	<i>Low</i>	Minimal	Low	Low	Low	Medium
	<i>Minimal</i>	Minimal	Minimal	Minimal	Low	Low

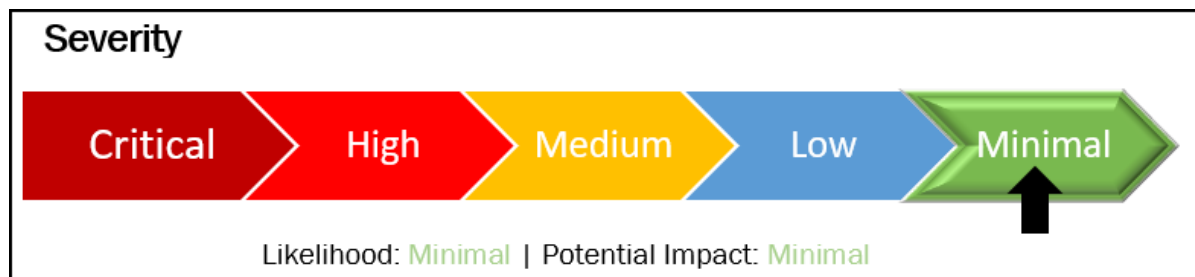
FINDINGS TABLE:

S.NO	HOST NAME	PORT NUMBER	CHECKLIST	CHECKED BY	DATE
			Remote Desktop Connection:		
			Remote desktop connection will be disabled on all systems to prevent unauthorized remote access.		
			Ctrl + Alt + Del:		
			The Ctrl + Alt + Del function will be enabled on the lock screen, ensuring that users must authenticate before any further actions are taken on the system.		
			Microsoft Store:		
			The Microsoft Store will be disabled to prevent the installation of unauthorized applications or software.		
			Command Prompt (CMD):		
			The CMD (Command Prompt) will be disabled to prevent users from executing potentially harmful or unauthorized commands on the system.		
			Snipping Tool:		
			The Snipping Tool will be disabled to restrict the ability to capture sensitive screen data or images.		
			Antivirus:		
			The antivirus software will be disabled only if explicitly approved or if managed through centralized security systems. No user-level disabling of antivirus will be allowed.		
			Approved Applications:		
			Only the following applications will be allowed on systems:		
			Google Chrome and Microsoft Office Suite (for supervisors only)		
			Excel 2007 (for approved users)		
			No other applications should be installed or accessible without prior approval from IT		

FINDING DETAILS:

Minimal Priority Findings:

1 – Sensitive Information Disclosure



Description:

This vulnerability occurs when sensitive information is inadvertently disclosed through an open network port, allowing unauthorized parties to access and potentially exploit this information.

Consequence:

Attackers can use this information to compromise the security of the system and potentially steal confidential data or disrupt services.

Instances:

- 1) Location – ASANSOL
- 2) Process – Swiggy

SR.NO	HOSTNAME	GROUP	POLICY	DOMIN	Serial No	STATUS	UPDATE DATE
1	BPOCSWGASN-0078	Asansol	Asansol	BPOCSWGASN.COM	2J8G202	ACTIVE	01-Feb-25
2	BPOCSWGASN-712	Asansol	Asansol	BPOCSWGASN.COM	FK3D3Y1	ACTIVE	01-Feb-25
3	BPOCSWGASN-711	Asansol	Asansol	BPOCSWGASN.COM	36JXBY1	ACTIVE	01-Feb-25
4	BPOCSWGASN-0059	Asansol	Asansol	BPOCSWGASN.COM	JR7NSZZ	ACTIVE	01-Feb-25
5		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
6	ASNSWG-CHAT-03	Asansol	Asansol	BPOCSWGASN.COM	5N2GJY1	ACTIVE	01-Feb-25
7	BPOCSWGASN-0042	Asansol	Asansol	BPOCSWGASN.COM	71KK52Z	ACTIVE	01-Feb-25
8	BPOCSWGASN-0094	Asansol	Asansol	BPOCSWGASN.COM	53HJFX1	ACTIVE	01-Feb-25
9	NEWBPOCSWG-0709	Asansol	Asansol	BPOCSWGASN.COM	BLK3HZ1	ACTIVE	01-Feb-25
10	BPOCSWGNEW-32	Asansol	Asansol	BPOCSWGASN.COM	HFKLSW1	ACTIVE	01-Feb-25
11		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25

12	BPOCSWGASA-072	Asansol	Asansol	BPOCSWGASN.COM	2WGDX1	ACTIVE	01-Feb-25
13	BPOCSWGASN-713	Asansol	Asansol	BPOCSWGASN.COM	54ZODY1	ACTIVE	01-Feb-25
14	BPOCSWGASN-0047	Asansol	Asansol	BPOCSWGASN.COM	7J1R8X1	ACTIVE	01-Feb-25
15	BPOCSWGASN-220	Asansol	Asansol	BPOCSWGASN.COM	8NPQFY1	ACTIVE	01-Feb-25
16		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
17	BPOCSWGASN-0051	Asansol	Asansol	BPOCSWGASN.COM	DY5QF2S	ACTIVE	01-Feb-25
18		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
19	BPOCSWGASN-8120	Asansol	Asansol	BPOCSWGASN.COM	D9W5RW1	ACTIVE	01-Feb-25
20	BPOC-CHAT-714	Asansol	Asansol	BPOCSWGASN.COM	HJ48GY1	ACTIVE	01-Feb-25
21	BPOCSWGASAN-0057	Asansol	Asansol	BPOCSWGASN.COM	9DCRDZ1	ACTIVE	01-Feb-25
22	BPOC-SWG-ASN-732	Asansol	Asansol	BPOCSWGASN.COM	JGQ8412	ACTIVE	01-Feb-25
23	SWGASN-CHAT-10	Asansol	Asansol	BPOCSWGASN.COM	4V5DZY1	ACTIVE	01-Feb-25
24	BPOCSWGASN-724	Asansol	Asansol	BPOCSWGASN.COM	CZ0SYX1	ACTIVE	01-Feb-25
25		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
26	BPOCSWGASN-58	Asansol	Asansol	BPOCSWGASN.COM	J3P9W12	ACTIVE	01-Feb-25
27	BPOCSWGASN-0071	Asansol	Asansol	BPOCSWGASN.COM	8620HX1	ACTIVE	01-Feb-25
28	BPOCSWGASN-728	Asansol	Asansol	BPOCSWGASN.COM	8LPMHT1	ACTIVE	01-Feb-25
29	BPOC-SWG-0010	Asansol	Asansol	BPOCSWGASN.COM	MJAVXMP	ACTIVE	01-Feb-25
30	BPOCSWGASN-0067	Asansol	Asansol	BPOCSWGASN.COM	FL4CCY1	ACTIVE	01-Feb-25
31	BPOCSWGASN-0046	Asansol	Asansol	BPOCSWGASN.COM	752MHT1	ACTIVE	01-Feb-25
32	BPOCSWGASN-732	Asansol	Asansol	BPOCSWGASN.COM	GVVTNW1	ACTIVE	01-Feb-25
33	ASNSWG-CHAT-04	Asansol	Asansol	BPOCSWGASN.COM	8LK3HZ1	ACTIVE	01-Feb-25
34	BPOCSWGASN-0083	Asansol	Asansol	BPOCSWGASN.COM	G32MP02	ACTIVE	01-Feb-25
35	BPOCSWGASN-210	Asansol	Asansol	BPOCSWGASN.COM	5LK3HZ1	ACTIVE	01-Feb-25
36	BPOCSWGASN-738	Asansol	Asansol	BPOCSWGASN.COM	9M1ZGZ1	ACTIVE	01-Feb-25
37		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
38	BPOCSWGASN-063	Asansol	Asansol	BPOCSWGASN.COM	9JVSDX1	ACTIVE	01-Feb-25
39	BPOCSWGASN-0076	Asansol	Asansol	BPOCSWGASN.COM	8095S22	ACTIVE	01-Feb-25
40		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
41	BPOCSWGASN-741	Asansol	Asansol	BPOCSWGASN.COM	F1BMZZ1	ACTIVE	01-Feb-25
42	ASN-SWG-CHAT-10	Asansol	Asansol	BPOCSWGASN.COM	HB2KJ02	ACTIVE	01-Feb-25
43	BPOCSWGASN-177	Asansol	Asansol	BPOCSWGASN.COM	65ST4W1	ACTIVE	01-Feb-25
44	BPOCSWGASN-0081	Asansol	Asansol	BPOCSWGASN.COM	8T9JGX1	ACTIVE	01-Feb-25
45	BPOCSWGASN-745	Asansol	Asansol	BPOCSWGASN.COM	93L7W31	ACTIVE	01-Feb-25
46	BPOCSWGASN-746	Asansol	Asansol	BPOCSWGASN.COM	5GMNF2S	ACTIVE	01-Feb-25
47	BPOCSWGASA-747	Asansol	Asansol	BPOCSWGASN.COM	BQWX241	ACTIVE	01-Feb-25
48	BPOCSWGASN-748	Asansol	Asansol	BPOCSWGASN.COM	4C3Vfy1	ACTIVE	01-Feb-25

49	ASNSWG-CHAT-14	Asansol	Asansol	BPOCSWGASN.COM	3K3V FY1	ACTIVE	01-Feb-25
50		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
51	BPOCSWGASN-751	Asansol	Asansol	BPOCSWGASN.COM	B2L0HY1	ACTIVE	01-Feb-25
52	BPOCSWGASA-0750	Asansol	Asansol	BPOCSWGASN.COM	DYJDFX1	ACTIVE	01-Feb-25
53	BPOCSWGNEW-31	Asansol	Asansol	BPOCSWGASN.COM	8VNHJY1	ACTIVE	01-Feb-25
54	BPOCSWGASN-0049	Asansol	Asansol	BPOCSWGASN.COM	GWLZM22	ACTIVE	01-Feb-25
55	BPOCSWGNEW-200	Asansol	Asansol	BPOCSWGASN.COM	DLFMZZ1	ACTIVE	01-Feb-25
56	BPOCSWGNEW-757	Asansol	Asansol	BPOCSWGASN.COM	GVX1RW1	ACTIVE	01-Feb-25
57	BPOCSWGASN-0055	Asansol	Asansol	BPOCSWGASN.COM	1K7N522	ACTIVE	01-Feb-25
58	BPOCSWGASN-758	Asansol	Asansol	BPOCSWGASN.COM	1D86VV1	ACTIVE	01-Feb-25
59	BPOCSWGASN-0053	Asansol	Asansol	BPOCSWGASN.COM	4Z3T8X1	ACTIVE	01-Feb-25
60		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
61	BPOCSWGASN-0074	Asansol	Asansol	BPOCSWGASN.COM	Z9XTWV1	ACTIVE	01-Feb-25
62	BPOCSWGASN-818	Asansol	Asansol	BPOCSWGASN.COM	CVPNZZ1	ACTIVE	01-Feb-25
63	BPOCSWGASN-763	Asansol	Asansol	BPOCSWGASN.COM	54J55W1	ACTIVE	01-Feb-25
64	BPOCSWGNEW-220	Asansol	Asansol	BPOCSWGASN.COM	BGFMZZ1	ACTIVE	01-Feb-25
65	BPOCASNNEW-01	Asansol	Asansol	BPOCSWGASN.COM	20PMZZ1	ACTIVE	01-Feb-25
66	BPOCSWGASN-767	Asansol	Asansol	BPOCSWGASN.COM	8PJ13Y1	ACTIVE	01-Feb-25
67	BPOCSWGNEW-21	Asansol	Asansol	BPOCSWGASN.COM	FG0VDX1	ACTIVE	01-Feb-25
68	BPOCSWGASN-0069	Asansol	Asansol	BPOCSWGASN.COM	C79HN22	ACTIVE	01-Feb-25
69	BPOCSWGASN-	Asansol	Asansol	BPOCSWGASN.COM	80KKBX1	ACTIVE	01-Feb-25
70	BPOCSWGASN-770	Asansol	Asansol	BPOCSWGASN.COM	70QB9X1	ACTIVE	01-Feb-25
71		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
72	BPOCSWGASN-772	Asansol	Asansol	BPOCSWGASN.COM	PBVPKE1	ACTIVE	01-Feb-25
73	BPOCSWGASN-773	Asansol	Asansol	BPOCSWGASN.COM	3MPQFY1	ACTIVE	01-Feb-25
74		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
75	BPOCSWGASN-8012	Asansol	Asansol	BPOCSWGASN.COM	3KDG302	ACTIVE	01-Feb-25
76	BPOCSWGASN-270	Asansol	Asansol	BPOCSWGASN.COM	JVKJGY1	ACTIVE	01-Feb-25
77	BPOCSWGASN-0031	Asansol	Asansol	BPOCSWGASN.COM	10DR4W1	ACTIVE	01-Feb-25
78	BPOCSWGASN-0778	Asansol	Asansol	BPOCSWGASN.COM	8TTXV12	ACTIVE	01-Feb-25
79	ASNSWG-CHAT-05	Asansol	Asansol	BPOCSWGASN.COM	3Z9MZZ1	ACTIVE	01-Feb-25
80	BPOCSWGASN-00048	Asansol	Asansol	BPOCSWGASN.COM	98K6G25	ACTIVE	01-Feb-25
81	BPOCSWGASN-781	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
82		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
83	BPOCSWGASN-816	Asansol	Asansol	BPOCSWGASN.COM	CHL7PV1	ACTIVE	01-Feb-25
84	BPOCSWGNEW-080	Asansol	Asansol	BPOCSWGASN.COM	3F3NJ02	ACTIVE	01-Feb-25
85	BPOCASNNEW-18	Asansol	Asansol	BPOCSWGASN.COM	D3806Z1	ACTIVE	01-Feb-25
86		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
87	BPOCSWGASN-180	Asansol	Asansol	BPOCSWGASN.COM	42QKMV1	ACTIVE	01-Feb-25

88	BPOCSWGASN-788	Asansol	Asansol	BPOCSWGASN.COM	JKVKZV1	ACTIVE	01-Feb-25
89	BPOCSWGNEW-35	Asansol	Asansol	BPOCSWGASN.COM	8DKKYBX	ACTIVE	01-Feb-25
90	BPOCSWGASN-201	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
91	BPOCSWGNEW-33	Asansol	Asansol	BPOCSWGASN.COM	9J4YR12	ACTIVE	01-Feb-25
92		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
93	BPOCSWGASN-980	Asansol	Asansol	BPOCSWGASN.COM	GY5QF2X	ACTIVE	01-Feb-25
94	BPOCSWGASN-0026	Asansol	Asansol	BPOCSWGASN.COM	DZ5C5W1	ACTIVE	01-Feb-25
95	BPOCSWGASN-798	Asansol	Asansol	BPOCSWGASN.COM	CQ0KZ1	ACTIVE	01-Feb-25
96	BPOCSWGASN-807	Asansol	Asansol	BPOCSWGASN.COM	3WPQFY1	ACTIVE	01-Feb-25
97	BPOCSWGASN-0087	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
98	BPOCSWGASN-30	Asansol	Asansol	BPOCSWGASN.COM	826KR12	ACTIVE	01-Feb-25
99		Asansol	Asansol	BPOCSWGASN.COM		NA	01-Feb-25
100	BPOCSWGASN-0077	Asansol	Asansol	BPOCSWGASN.COM	6LWQBZ1	ACTIVE	01-Feb-25
101	BPOCSWGASN-792	Asansol	Asansol	BPOCSWGASN.COM	7PX48X1	ACTIVE	01-Feb-25
102	BPOCSWGNEW-065	Asansol	Asansol	BPOCSWGASN.COM	8T4KM22	ACTIVE	01-Feb-25
103	SWGASN-TRN2-01	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
104	BPOCSWGASN-251	Asansol	Asansol	BPOCSWGASN.COM	DXVCQW1	ACTIVE	01-Feb-25
105	BPOCASNNEW-808	Asansol	Asansol	BPOCSWGASN.COM	C36KR12	ACTIVE	01-Feb-25
106	BPOCSWGASN-183	Asansol	Asansol	BPOCSWGASN.COM	FTV47V1	ACTIVE	01-Feb-25
107	BPOCSWGASN-797	Asansol	Asansol	BPOCSWGASN.COM	BRPQFY1	ACTIVE	01-Feb-25
108	BPOCSWGASN-805	Asansol	Asansol	BPOCSWGASN.COM	7BM9YV1	ACTIVE	01-Feb-25
109	BPOCSWGASN-0028	Asansol	Asansol	BPOCSWGASN.COM	96GF5W1	ACTIVE	01-Feb-25
110	BPOCSWGASN-250	Asansol	Asansol	BPOCSWGASN.COM	6DF44W1	ACTIVE	01-Feb-25
111	BPOCSWGASN-186	Asansol	Asansol	BPOCSWGASN.COM	3FKJJ02	ACTIVE	01-Feb-25
112	BPOCSWGASN-819	Asansol	Asansol	BPOCSWGASN.COM	4PY9TW1	ACTIVE	01-Feb-25
113	BPOCSWGASN-825	Asansol	Asansol	BPOCSWGASN.COM	BRFWK02	ACTIVE	01-Feb-25
114	BPOCSWGASN-820	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
115	SWG-TRAINER-ASN	Asansol	Asansol	BPOCSWGASN.COM	7GL7PV1	ACTIVE	01-Feb-25
116	BPOC-SWG-0017	Asansol	Asansol	BPOCSWGASN.COM	GNP9BY1	ACTIVE	01-Feb-25
117	SWGASN-147	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
118	BPOC-SWG-0008	Asansol	Asansol	BPOCSWGASN.COM	MJPZZCN	ACTIVE	01-Feb-25
119	SWG-ASN-TR2-10	Asansol	Asansol	BPOCSWGASN.COM	BNWK22S	ACTIVE	01-Feb-25
120	SWGASN-122	Asansol	Asansol	BPOCSWGASN.COM	L94WZ40	ACTIVE	01-Feb-25
121	BPOC-SWG-0011	Asansol	Asansol	BPOCSWGASN.COM	PBLEW11	ACTIVE	01-Feb-25
122	SWGASN-148	Asansol	Asansol	BPOCSWGASN.COM	6CJ062S	ACTIVE	01-Feb-25
123	SWG-ASN-TR2-06	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
124	SWGASN-129	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
125	SWGASN-126	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
126	SWGASN-127	Asansol	Asansol	BPOCSWGASN.COM	PBXHEBX	ACTIVE	01-Feb-25
127	SWGASN-136	Asansol	Asansol	BPOCSWGASN.COM	MJDLBNY	ACTIVE	01-Feb-25
128	SWGASN-130	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
129	SWGASN-128	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25

130	SWGASN-140	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
131	SWGASN-145	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
132	SWGASN-147	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25
133	SWGASN-121	Asansol	Asansol	BPOCSWGASN.COM	NA	ACTIVE	01-Feb-25

A detailed plan for closure of the gaps found during this review should be created. Network must be re-tested, before moving the new code into production environment. A periodic monitoring mechanism should be instituted to ensure compliance levels are maintained all the time. BPO Convergence Pvt Ltd. is happy to perform periodic assessments once in a quarter or whenever there is a major code change or when industry consortiums report new vulnerabilities or threats, whichever comes first.

APPENDIX 1: EXTERNAL NETWORK SECURITY ASSESSMENT TASK

An indicative list of tasks conducted for a web application assessment, in addition to the application's requirements;

- ✓ **Vulnerability Scanning** – Using automated tools to scan the target network for known vulnerabilities, which can include outdated software, unpatched systems, and misconfigured devices.
- ✓ **Network Mapping** - Mapping the network to identify all devices and systems on the network, including their IP addresses, operating systems, and services running.
- ✓ **Port Scanning** - Using automated tools to scan all open ports on the target network to identify any unauthorized services, applications or open ports that may be vulnerable to attack.
- ✓ **Exploitation Testing**: Testing for exploitable vulnerabilities identified during the vulnerability scanning and port scanning phases using manual and automated tools to verify their existence.
- ✓ **Password Cracking**: Testing the strength of passwords used within the network and identifying any weak or easily guessable passwords which can be used to gain unauthorized access.
- ✓ **Firewall Testing**: Testing the security of the firewall configuration to identify any misconfigured rules or policies that may be exploited.
- ✓ **Denial of Service (DoS) Testing**: Testing the resilience of the network against

Denial-of-Service attacks that can cause network outages.

ABOUT US

BPO Convergence Pvt. Ltd., a Fornax Company, is a Business Process Management (BPM) company specializing in customer experience management, managed services, analytics, staffing solutions, and transaction processing, with a focus on delivering cost-effective and sustainable solutions

For more information, visit us at www.bpoconvergence.com