

BPO Convergence

Monthly IT Evaluation & Testing Report

Wednesday, 23 July 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	
Assessment ID	RAPIDO_Internal_Network_V4.2-
Application Type	Internal Network
Authors	Sundaraiah
Penetration Tester	Sundar & Satya
Report Version	4.2
Last Update	24/07/2025

ASSESSMENT SCOPE SUMMARY

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

In scope Network Name	RAPIDO 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.

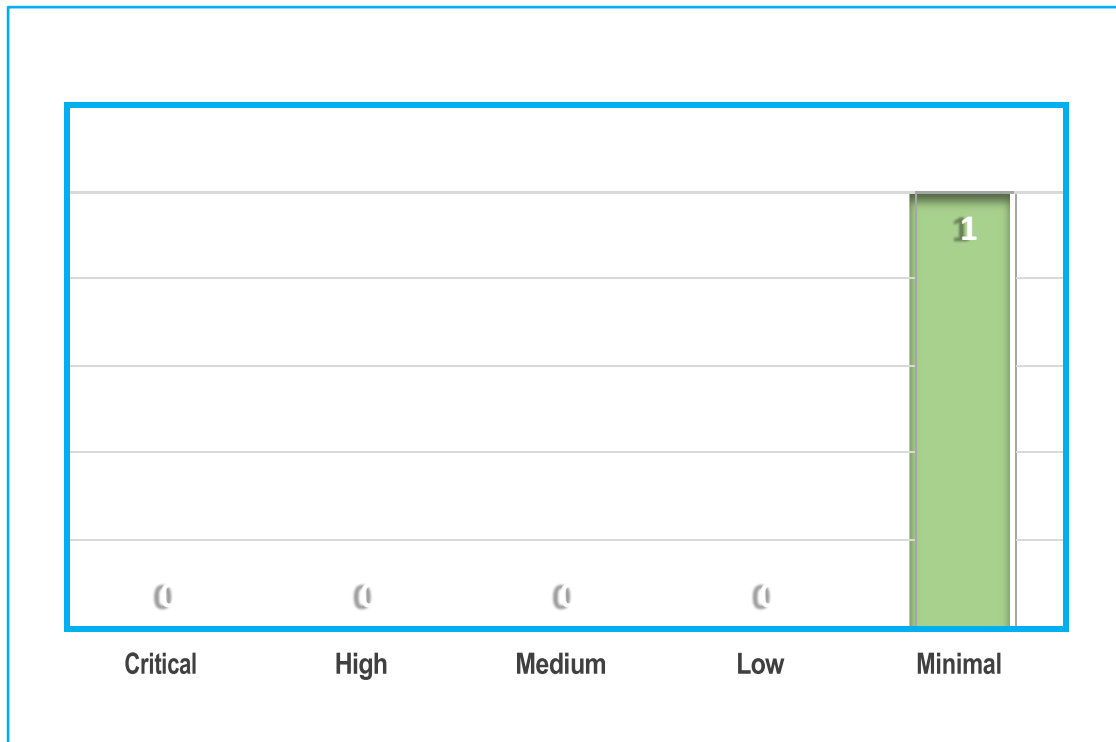
To evaluate the security of the network and network, IT team attempted to perform unauthorized transactions, obtain confidential information, and determine the overall security of the network by performing a wide variety of vulnerability checks.

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.c 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 described security vulnerability 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 the vulnerability or the vulnerability is very obvious and easily accessible.

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

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

Minimal: Adversaries are highly unlikely to leverage the vulnerability.

Impact

The impact the vulnerability would have on the organization if it were successfully exploited is rated with the following values:

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

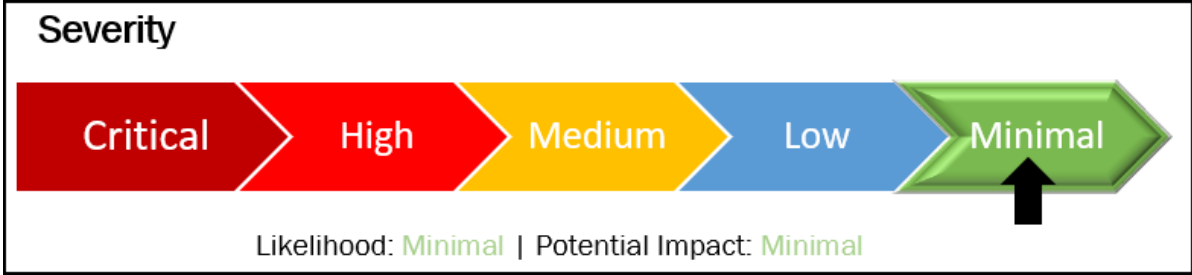
FINDINGS TABLE:

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 – Hyderabad

Process- RAPIDO

S.NO	END POINT NAME	GROUP	POLICY	DOMIN	STATUS	DATABASE UPDATE DATE
1	HR1.	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
2	RPD-TR- 01	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
3	RPD-TR- 02	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
4	RPD-TR-04	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
5	RPD-TR- 05	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
6	RPD-TR-007	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
7	RPD-TR-03	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
8	RPD-WS-001	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
9	RPD-WS-0011	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
10	RPD-WS-006	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
11	RPD-WS-007	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
12	RPD-WS-009	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
13	RPD-WS-010	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
14	RPD-WS-011	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
15	RPD-WS-012	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25

16	RPD-WS-013	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
17	RPD-WS-014	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
18	RPD-WS-015	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
19	RPD-WS-016	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
20	RPD-WS-017	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
21	RPD-WS-018	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
22	RPD-WS-019	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
23	RPD-WS-020	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
24	RPD-WS-021	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
25	RPD-WS-022	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
26	RPD-WS-0221	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
27	RPD-WS-023	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
28	RPD-WS-024	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
29	RPD-WS-025	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
30	RPD-WS-026	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
31	RPD-WS-027	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
32	RPD-WS-028	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
33	RPD-WS-029	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
34	RPD-WS-030	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
35	RPD-WS-031	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
36	RPD-WS-032	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
37	RPD-WS-033	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
38	RPD-WS-034	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
39	RPD-WS-035	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
40	RPD-WS-036	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
41	RPD-WS-037	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
42	RPD-WS-038	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
43	RPD-WS-039	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
44	RPD-WS-040	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
45	RPD-WS-041	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
46	RPD-WS-042	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
47	RPD-WS-043	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
48	RPD-WS-044	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
49	RPD-WS-045	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
50	RPD-WS-046	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
51	RPD-WS-047	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
52	RPD-WS-048	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
53	RPD-WS-049	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
54	RPD-WS-050	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
55	RPD-WS-051	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
56	RPD-WS-052	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
57	RPD-WS-053	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
58	RPD-WS-054	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
59	RPD-WS-056	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
60	RPD-WS-057	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
61	RPD-WS-058	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25

62	RPD-WS-059	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
63	RPD-WS-060	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
64	RPD-WS-061	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
65	RPD-WS-063	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
66	RPD-WS-064	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
67	RPD-WS-065	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
68	RPD-WS-066	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
69	RPD-WS-067	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
70	RPD-WS-068	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
71	RPD-WS-069	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
72	RPD-WS-070	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
73	RPD-WS-071	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
74	RPD-WS-073	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
75	RPD-WS-074	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
76	RPD-WS-075	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
77	RPD-WS-076	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
78	RPD-WS-077	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
79	RPD-WS-078	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
80	RPD-WS-080	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
81	RPD-WS-081	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
82	RPD-WS-082	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
83	RPD-WS-083	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
84	RPD-WS-084	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
85	RPD-WS-085	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
86	RPD-WS-086	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
87	RPD-WS-088	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
88	RPD-WS-089	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
89	RPD-WS-090A	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
90	RPD-WS-091	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
91	RPD-WS-092	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
92	RPD-WS-093	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
93	RPD-WS-094	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
94	RPD-WS-095	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
95	RPD-WS-096	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
96	RPD-WS-097	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
97	RPD-WS-098	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
98	RPD-WS-099	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
99	RPD-WS-100	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
100	RPD-WS-101	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
101	RPD-WS-102	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
102	RPD-WS-103	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
103	RPD-WS-104	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
104	RPD-WS-105	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
105	RPD-WS-106	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
106	RPD-WS-108	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
107	RPD-WS-109	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25

108	RPD-WS-110	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
109	RPD-WS-113	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
110	RPD-WS-114	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
111	RPD-WS-115	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
112	RPD-WS-116	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
113	RPD-WS-117	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
114	RPD-WS-118	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
115	RPD-WS-119	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
116	RPD-WS-120	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
117	RPD-WS-122	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
118	RPD-WS-123	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
119	RPD-WS-123A	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
120	RPD-WS-124	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
121	RPD-WS-125	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
122	RPD-WS-126	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
123	RPD-WS-127	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
124	RPD-WS-132	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
125	RPD-WS-135	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
126	RPD-WS-145	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
127	RPD-WS-146	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
128	RPD-WS-147	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
129	RPD-WS-150A	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
130	RPD-WS-152	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
131	RPD-WS-153	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
132	RPD-WS-154	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
133	RPD-WS-155	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
134	RPD-WS-156	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
135	RPD-WS-157	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
136	RPD-WS-159	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
137	RPD-WS-160	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
138	RPD-WS-161	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
139	RPD-WS-162	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
140	RPD-WS-163	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
141	RPD-WS-164	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
142	RPD-WS-165	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
143	RPD-WS-166	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
144	RPD-WS-167	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
145	RPD-WS-167A	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
146	RPD-WS-168	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
147	RPD-WS-169	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
148	RPD-WS-170	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
149	RPD-WS-171	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
150	RPD-WS-172	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
151	RPD-WS-173	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
152	RPD-WS-174	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
153	RPD-WS-175	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25

154	RPD-WS-175A	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
155	RPD-WS-176	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
156	RPD-WS-177	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
157	RPD-WS-177A	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
158	RPD-WS-178	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
159	RPD-WS-178A	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
160	RPD-WS-179	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
161	RPD-WS-180	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
162	RPD-WS-180A	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
163	RPD-WS-181A	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
164	RPD-WS-182	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
165	RPD-WS-183	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
166	RPD-WS-184	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
167	RPD-WS-184A	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
168	RPD-WS-187	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
169	RPD-WS-197	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
170	RPD-WS-208	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
171	RPD-WS-214	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
172	RPD-WS-220	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
173	RPD-WS-248	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
174	RPD-WS-250	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
175	RPD-WS-251	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
176	RPD-WS-255	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
177	RPD-WS-256	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
178	RPD-WS-257	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
179	RPD-WS-258	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
180	RPD-WS-286	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
181	RPD-WS-62	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
182	RPD-WS-90	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
183	RPD-WS-134	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
184	RPD-WS-QACCC1	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
185	RPD-WS-QASUPPLY	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
186	RPD-QA-SUP	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
187	SUP-TRAINER	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
188	RPD-WS-RTQM	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
189	MIS-RAPIDO	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
190	RPD-WS-RENTRA	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
191	RPD-WS-QACCC2	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25
192	RPD-WS-QACCC3	RAPIDO	RAPIDO	BPOCHYD.COM	ACTIVE	23-July-25

WAY AHEAD:

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