



# WEB APPLICATION PENETRATION TESTING (WAPT) REPORT



Submitted to:



**Bangla Sahayata Kendra**



EMPANELLED ORGANIZATION

**GOVERNANCE, RISK & COMPLIANCE | MANAGED SECURITY SERVICES**

## Document Control

<b>Document type</b>	Web Application Penetration Testing (WAPT) Report of URL: <a href="https://bsk.wb.gov.in/">https://bsk.wb.gov.in/</a> for Bangla Sahayata Kendra.
<b>Document owner</b>	Prime Infoserv LLP

<b>Authors &amp; Auditors</b>	<b>Mail ID</b>
Mr. Bijoy Sonari	<a href="mailto:bijoy@primeinfoserv.com">bijoy@primeinfoserv.com</a>

<b>Reviewed &amp; verified by</b>	<b>Mail ID</b>
Mr. Pallav Rohatgi	<a href="mailto:pallav@primeinfoserv.com">pallav@primeinfoserv.com</a>

<b>Approved by</b>	<b>Digital Signature</b>
Kiranjit Manna, CISA Certificate No. 18147519	

Revision History		
Version	Date	Description
1.0	28/05/2024	Web Application Penetration Testing (WAPT) Report of URL: <a href="https://bsk.wb.gov.in/">https://bsk.wb.gov.in/</a> for Bangla Sahayata Kendra.
1.1	12/06/2024	Revalidation for the same.

Assessment Information - Auditee			
Client	Bangla Sahayata Kendra		
Contact Person	Dr Arindam Ray		
Contact Number	+91 93507 78825	Mail ID	<a href="mailto:cto.bsk@wb.gov.in">cto.bsk@wb.gov.in</a>
Assessment Type	Web Application Penetration Testing (WAPT) Report of URL: <a href="https://bsk.wb.gov.in/">https://bsk.wb.gov.in/</a> for Bangla Sahayata Kendra.		
PO. No. & Date	46-PAR(BSK)/BSK-23/2023 & 09/05/2024		
Report Ref. No.	PIL/BSK/24-25/0112062024		
Assessment Period (Stage I & II)	13/05/2024 - 22/05/2024 & 10/06/2024 - 12/06/2024	Report Date (Stage I & II)	28/05/2024 & 12/06/2024

### Notice of Confidentiality

This document contains proprietary and confidential information of Prime Infoserv LLP. The recipient agrees to maintain this information in confidence and not to reproduce or to disclose this information to any person outside of the group directly responsible for the evaluation of its contents. There is no obligation to maintain the confidentiality of any information which was known to the recipient prior to the receipt of this document from Prime Infoserv LLP or which becomes publicly known through no fault of the recipient or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to Prime Infoserv LLP.

## Table of Contents

1. Executive Summary .....	4
2. Methodology & Approach .....	5
2.1. WAPT.....	8
2.1.1. Web Apps Audit Test Standard followed.....	9
3. Risk Level & Description .....	12
4. Tools used during assessment .....	12
5. Assessment Scope.....	12
6. Disclaimer .....	13
7. Assumptions .....	13
8. Executive Summary Report.....	14
9. Directions by CERT-In under section 70B, IT Act 2000 .....	15
10. About Prime.....	16
11. Audit Test Standard.....	16
12. Team Skill Set.....	16
13. Contact Us .....	17

CONFIDENTIAL

## 1. Executive Summary

The State Government of West Bengal has established 3561 Bangla Sahayata Kendras (BSKs) across the state to provide free government services at the grassroots level through online mode. The aim is to strengthen the existing system of information dissemination about various social and development schemes. The BSKs are strategically located in the offices of District Magistrates, Sub-Divisional Officers, Block Development Officers, Gram Panchayats, Health Centres, Government Aided Libraries, and all Urban Local Bodies (ULBs).

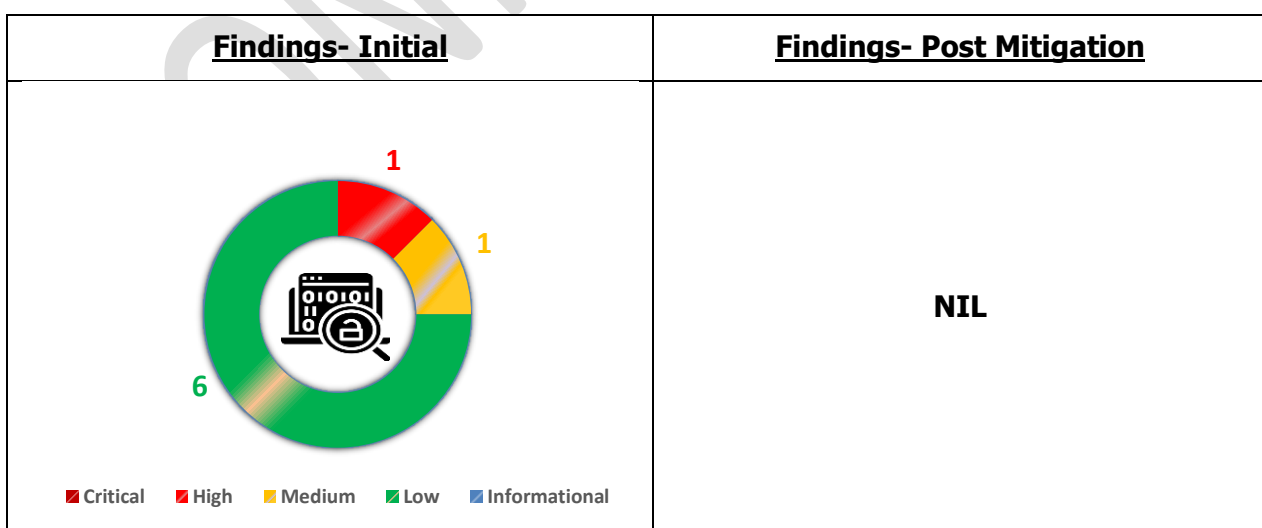
The BSKs offer 260 public services, including 104 transaction services, 97 eWallet services and 59 information services, from 40 different departments. The Personnel & Administrative Reforms and e-Governance Department of the Government of West Bengal is the Nodal Department coordinating the BSK project, while a Project Management Unit (PMU) at the state level oversees the day-to-day functioning of the BSKs. All the services offered by the BSKs can also be availed online through the portal <https://bsk.wb.gov.in/>. Notably, all BSK services are provided entirely free, and citizens are not required to pay any service charge to avail of the services.

Bangla Sahayata Kendra wanted to get the mentioned URL audited by a Cert-IN empanelled organisation.

Prime Infoserv LLP a Cert-IN empanelled organisation conducted the audit of mentioned URL and submitted detailed findings in phased manner. This report included all possible minute details of the outcomes against the scope, along with all significant findings and detailed remediation advice. This summary report provides a synopsis of the key findings and relates these backs to business impacts. The report covers not only the identified Gaps, but also the possible recommendations & blueprinting.

The graph below shows a summary of the number of vulnerabilities found for each impact level for the Vulnerabilities Assessment.

### OVERALL VULNERABILITIES



More insights will be illustrated through the executive summary sections.

## 2. Methodology & Approach

With the increasing number of cyber-attacks and data breaches affecting companies, the public now demands more from organizations in protecting the confidentiality, integrity and availability of sensitive data and systems.

Prime’s Cyber Risk Assessment will provide you with a clear snapshot of the effectiveness of your current cyber security measures and your preparedness in managing cyber risks. Starting with a high-level assessment with the Board and Audit Committee as interested stakeholders of the report, we then draw on our “cyber capability library” – a set of security capability indicators, which your investors, customers and regulators would be keen to understand. This will enable you to visualize your current security posture and identify hidden gaps to be investigated and mitigated.

***We view your cyber security from different dimensions.***



*Prioritise your plans to combat cyber security risks*

*Provide insights on your posture and capabilities with reference to industry standards*

*Assess your ability to handle massive cyber attacks*

*Evaluate the latest threat landscape you are facing*

### Focusing on nine key areas



### Our Journey together with you

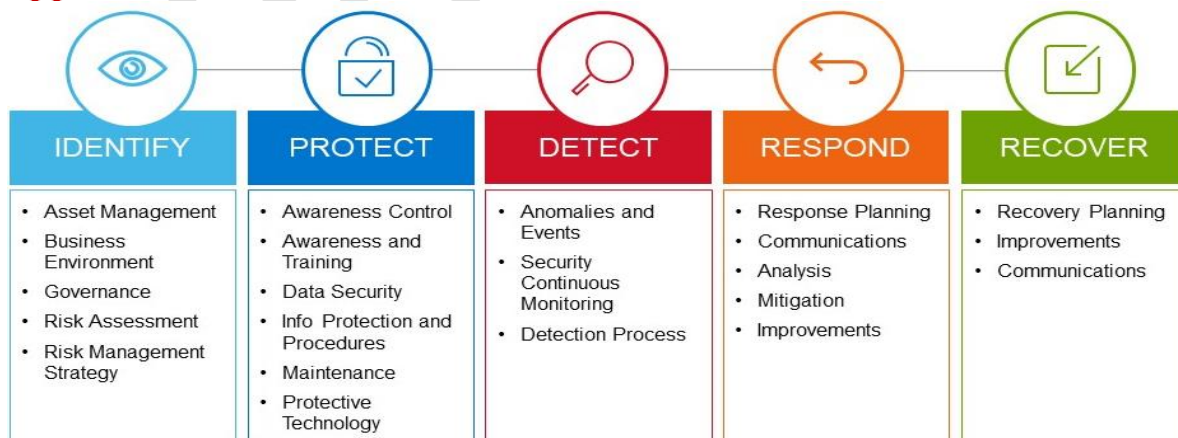


### Developing a path to enhance cyber security posture

Our recommendations are prioritised based on the analysis of various factors e.g. benefits/impacts and ease of action, to formulate a roadmap with progressive stages of implementation. This helps you mitigate the cyber risks you are facing and achieve your target state of readiness.



### Approach at a Glance



## ***Framework***

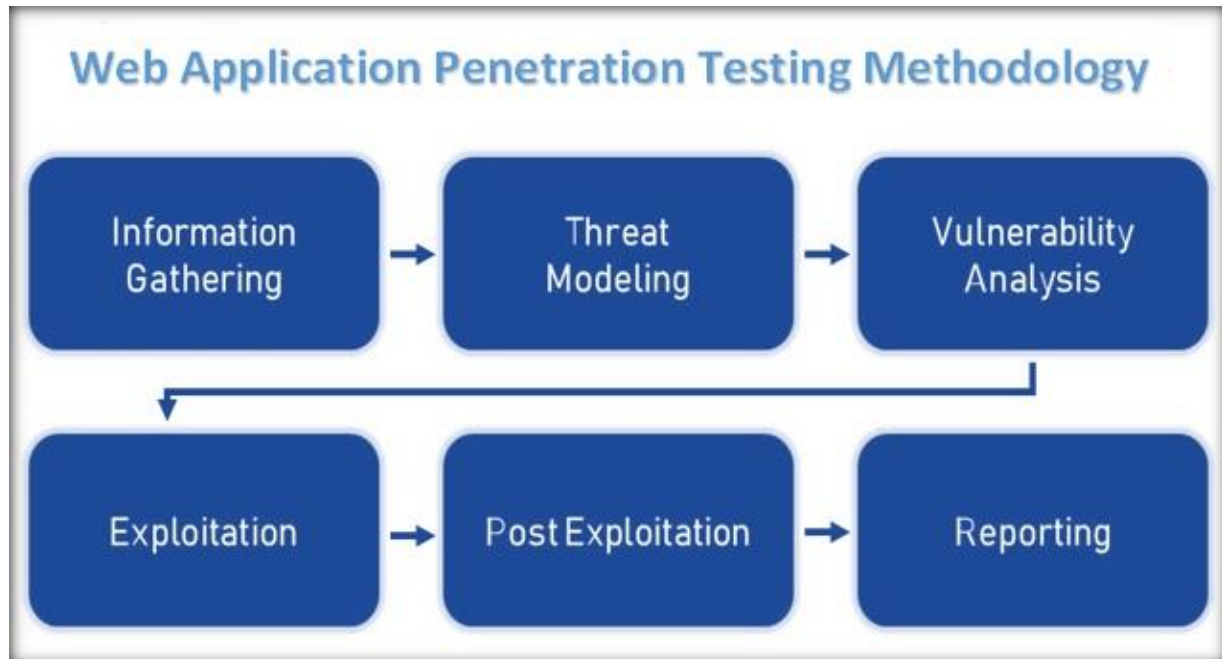
Cyber security frameworks are sets of documents describing guidelines, standards, and best practices designed for cyber security risk management. The frameworks exist to reduce an organization's exposure to weaknesses and vulnerabilities that hackers and other cyber criminals may exploit.

For further details, refer to the link: <https://www.nist.gov/cyberframework>

CONFIDENTIAL

## 2.1. WAPT

### Our present Web Application Audit Plan involves



- **Information Gathering**

Gathering of required information through mutual discussion & verifying of same through various tools under OSINT techniques. Required information has been gathered using NMAP & OSINT. The first phase in security assessment is focused on collecting as much information as possible about a target application. We start information gathering by using OSINT techniques.

- **Technical Analysis**

Analysing of web site from a technical perspective to check performance bottlenecks if any. To check if there are any technical faults that is preventing your web site from performing.

- **Vulnerability Assessment**

Vulnerability assessment is the process of identifying of vulnerabilities and classifying as defined and prioritizing vulnerabilities in Web Application.

- **Penetration Testing**

Web application penetration testing is the process of verifying vulnerabilities identified. Using penetration testing techniques on a web application to exploits all identified vulnerabilities.

- **Reporting**

Preparation of report as per severity along with remedial recommendation. Evidence against claims and recommendation after successfully exploit all vulnerabilities, we prepare detailed report including Proof of concept and recommendations.

### 2.1.1. Web Apps Audit Test Standard followed

#### ➤ OWASP Top 10 (2021)

The Open Web Application Security Project (OWASP) is a non-profit community of software developers, engineers, and freelancers that provides resources and tools for web application security. Every few years, OWASP releases a report on the 10 most critical web application security risks.

We follow OWASP Top 10 vulnerabilities for testing for vulnerabilities. For more details, refer to the following link:

<https://owasp.org/www-project-top-ten/>

#### ➤ OWASP Top 10 (2021) Vulnerability Categories and Impact

S. No.	Vulnerability Categories	Impact
A01	<p><b>Broken Access Control</b></p> <p>Broken Access Control happens when access permissions are misconfigured thereby allowing attackers to access, modify or delete data, files and accounts that they should not have access to in the first place.</p>	<p>Attackers can exploit authorization flaws to accomplish the following:</p> <ul style="list-style-type: none"> <li>• Access unauthorized functionality and/or data</li> <li>• View sensitive files</li> <li>• Change access rights</li> <li>• Edit files and records</li> </ul>
A02	<p><b>Cryptographic Failures</b></p> <p>Cryptographic failures occur when sensitive data is insufficiently protected and therefore leaked or exposed to unauthorized audiences. Such failures are most common if data is transmitted or stored in clear text or using known-to-be-weak cryptographic algorithms such as MD5 or SHA-1.</p>	<p>An attacker monitors network traffic (e.g., at an insecure wireless network), downgrades connections from HTTPS to HTTP, intercepts requests, and steals the user's session cookie. The attacker then replays this cookie and hijacks the user's (authenticated) session, accessing or modifying the user's private data. Instead of the above, they could alter all transported data.</p>
A03	<p><b>Injection</b></p> <p>An attacker can execute unintended commands or gain access to sensitive data by injecting malicious data as part of a command or query. This usually happens when a website fails to filter, validate or sanitize users' inputs or implement parameterization.</p>	<p>Injection vulnerabilities can occur when a query or command is used to insert untrusted data into the interpreter via SQL, OS, NoSQL, or LDAP injection. The hostile data injected through this attack vector tricks the interpreter to make the application do something it was not designed for, such as generating unintended commands or accessing data without proper authentication.</p>

S. No.	Vulnerability Categories	Impact
A04	<p><b>Insecure Design</b></p> <p>Insecure design is a new entry on the OWASP Top 10 in 2021. It is different from insecure implementation in that it has more to do with risks related to design and architectural flaws. A secure implementation might have an insecure design which still renders a web application vulnerable to attacks and exploits.</p>	<p>Applications that were not developed with security in mind from the very beginning are more likely to put user data and security at risk, and require updates, patches, and fixes to prevent these risks. Applications without secure design are low hanging fruit for attackers and can cost incalculable sums of damage in terms of leaked data, tarnished reputations, and paid working-hours of cleanup and future prevention.</p>
A05	<p><b>Security Misconfiguration</b></p> <p>This category covers a brand range of potential vulnerabilities including insecure default configurations, incomplete configurations, and misconfigured HTTP headers, using insecure default usernames and passwords, etc.</p>	<p>There are many types of misconfigurations that expose the company to cybersecurity risk, including:</p> <ul style="list-style-type: none"> <li>• Accepting default settings that are insecure</li> <li>• Overly accessible cloud storage resources</li> <li>• Incomplete configurations</li> <li>• Misconfigured HTTP headers</li> <li>• Verbose error messages that contain sensitive information</li> </ul>
A06	<p><b>Vulnerable and Outdated Components</b></p> <p>This refers to known issues where vulnerabilities exist because developers either do not know the versions of components used including those of nested dependencies, or are not aware that the software used is already unsupported or out of date.</p>	<p>Any component with a known vulnerability becomes a weak link that can impact the security of the entire application.</p>
A07	<p><b>Identification and Authentication Failures</b></p> <p>This category covers weaknesses in authentication and session management in web applications. The resulting vulnerabilities allow attackers to gain unauthorized access to accounts and/or data.</p>	<p>Websites with broken authentication vulnerabilities are very common on the web. Broken authentication usually refers to logic issues that occur on the application authentication's mechanism, like bad session management prone to username enumeration – when a malicious actor uses brute-force techniques to either guess or confirm valid users in a system.</p>

S. No.	Vulnerability Categories	Impact
<b>A08</b>	<p><b>Software and Data Integrity Failures</b></p> <p>It is concerned with the failure to verify the integrity of software updates and patches prior to implementation on live applications and servers.</p>	<p>These failures can be summarized as follows:</p> <ul style="list-style-type: none"> <li>• Usage of code that does not verify integrity of source</li> <li>• Usage of third-party plugins where you do not control the source</li> <li>• Plugins and extensions from untrusted sources</li> <li>• The introduction of or potential for compromise or unauthorised access</li> <li>• Auto-updates assume trust of the source</li> </ul>
<b>A09</b>	<p><b>Security Logging and Monitoring Failures</b></p> <p>Logging and monitoring are essential components in ensuring that any suspicious activity can be detected close to real-time, or diagnosed after the fact. Failure to keep sufficient records in these areas could subsequently lead to slower incident responses, thereby accentuating the potential damages of breaches.</p>	<p>This window gives cyber thieves plenty of time to tamper with servers, corrupt databases, steal confidential information, and plant malicious code.</p>
<b>A10</b>	<p><b>Server-Side Request Forgery</b></p> <p>Server-Side Request Forgery (SSRF) occurs when a web application proceeds to fetch data without first validating user-supplied URL. In a bid to provide end-users with convenience, fetching data using a URL has become more common. The vulnerability allows an attacker to compel the web application to send a crafted request to unexpected destinations even when adequately protected by firewalls, VPNs and Network Access Control List (ACL).</p>	<p>When a web application fetches a remote resource without validating the user-supplied URL, an SSRF fault occurs. Even if the program is secured by a firewall, VPN, or another sort of network access control list, an attacker can force it to send a forged request to an unexpected location.</p>

### ➤ **CWE/SANS TOP 25 Most Dangerous Software Errors**

The CWE/SANS Top 25 is an important resource for programmers, including embedded developers. A majority of these security vulnerabilities apply to embedded systems, and Wind River has identified the most significant 10. Mitigation strategies are key to addressing the security risk to your device

We also follow SANS Top 25 Vulnerabilities. For more information about SANS top 25, refer to the following link:

<https://www.sans.org/top25-software-errors/>

### 3. Risk Level & Description

Vulnerabilities are categorized into different Severity ratings like Critical, High, Medium, Low and Informational. For more details, refer to the following link:

<https://nvd.nist.gov/vuln-metrics/cvss>

### 4. Tools used during assessment

We are using various commercial, open source and customized tools to conduct the WAPT. Following are few to mention.



### 5. Assessment Scope

Sl. No.	URL Details
1	<a href="https://bsk.wb.gov.in/">https://bsk.wb.gov.in/</a>

## 6. Disclaimer

This report is intended to provide a detailed overview of the completed Web Application Penetration Testing (WAPT) Report of URL: <https://bsk.wb.gov.in/> as per assessment scope of Bangla Sahayata Kendra, which describes the latest findings identified by Prime Infoserv LLP.

## 7. Assumptions

This report has been produced based on the output of the Security Assessment that was conducted on a particular date.

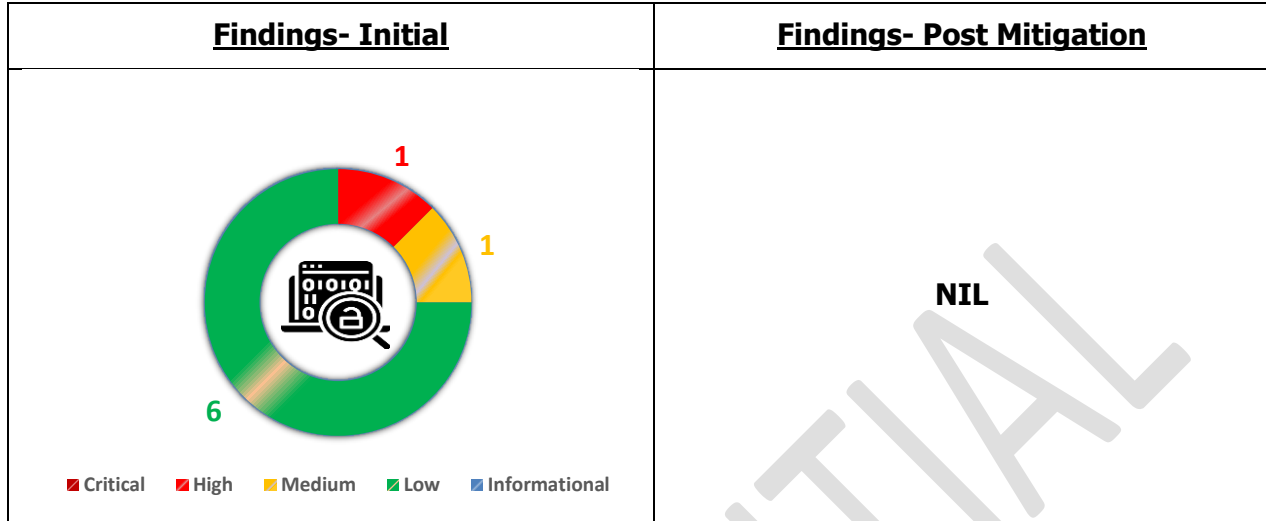
All vulnerabilities have been highlighted in the report assuming that the utilities and other applications installed on the systems were being used for the business purpose, and accordingly the recommendation to mitigate those vulnerabilities have been made. It is, therefore, recommended that prior to acting on the recommendation, following actions are taken:

- Ascertain whether a service or application for which vulnerability has been identified and recommendation is made is actually required in the system for business purpose. In case there is no requirement of such services or applications, the same may be removed or disabled following an appropriate process. Else, the recommendations are applied on the system.
- Appropriate backup and rollback plan to be made prior to implementing the recommendation on the system.
- Vulnerabilities identified were as on the date testing conducted and also as per the scan policies (intrusive or non-intrusive) & plugins selected. There may be vulnerabilities which may exist and may not assess, since their exploits may lead to system downtime due to Denial of Service (DOS) attack. Also, the vulnerabilities identified after the scan date may also not form part of this report.
- Informing Vulnerabilities identified to Computer Emergency Response Team (CERT-In) as per directives

Objectives	Status
Identification of <b>Vulnerabilities</b> in mentioned URL(s)	Completed ✓
<b>Reporting of Vulnerabilities</b>	Completed ✓

## 8. Executive Summary Report

### OVERALL VULNERABILITIES



#### Summary of Findings:

Sl. No.	Vulnerability Name	Vulnerability Risk Type	Revalidation Status
1	Out-of-date Version (Axios)	High	Fixed
2	Internal Server Error Leading to Information Disclosure	Medium	Fixed
3	Content Security Policy (CSP) Not Implemented	Low	Fixed
4	HTTP Strict Transport Security (HSTS) Policy Not Enabled		Fixed
5	Version Disclosure (Axios)		Fixed
6	Version Disclosure (Bootstrapjs)		Fixed
7	Version Disclosure (Highcharts)		Fixed
8	Version Disclosure (jQuery)		Fixed

## 9. Directions by CERT-In under section 70B, IT Act 2000

- Directions under subsection (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedures, preventions, response and reporting of cyber incidents for safe & trusted Internet (dated 24.04.2022) can be found here - [https://www.cert-in.org.in/PDF/CERT-In\\_Directions\\_70B\\_28.04.2022.pdf](https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf)
- Recommended Actions to be taken by the organizations are as followed
  - Synchronize the system times with NIC/NTP Time servers.
    - NPL India time server – [time.nplindia.org](http://time.nplindia.org)
    - NIC Time servers
      - [samay1.nic.in](http://samay1.nic.in)
      - [samay2.nic.in](http://samay2.nic.in)
  - Cyber incidents shall mandatorily report to CERT-In within 6 hours of noticing.
    - This can be done by email – [incident@cert-in.org.in](mailto:incident@cert-in.org.in)
    - Phone – 1800-11-4949
    - Fax – 1800-11-6969
    - Format of the report can be found at [www.cert-in.org.in](http://www.cert-in.org.in)
  - All ICT systems should have logs enabled and maintain them securely for a rolling period of 180 days. This should be provided to CERT-in along with the incident report.
- **Recommended to read the full direction, using the link mentioned above.**

## 10. About Prime

- A Global Specialised ICT, DC & Cyber Security Service Provider
- Founded by a Team of senior professionals with System Integration, Telecom, MNC & Govt. Background
- 350+ Global Clientele
- **ISO 9001, ISO 27001, ISO 22301** Certified Enterprise with **CERT-in** Empanelment
- Experienced in handling customers in National Critical Infra sector
- PMP Based Project Management and **ITIL** Based Service Operations
- Managed Services Capabilities with own **NOC & SOC** powered by best in class tools and round the clock specialized resources.
- Member of **NASSCOM-DSCI, Infosec Foundation, TiE, NCIIPC, CDAC, Webel, CTO Forum, Cyber Security Malaysia**



## 11. Audit Test Standard



## 12. Team Skill Set



### 13. Contact Us

<b>Office Contacts</b>	Phone : +91 33 4008 5677 Email : <a href="mailto:support@primeinfoserv.com">support@primeinfoserv.com</a> ; <a href="mailto:info@primeinfoserv.com">info@primeinfoserv.com</a>
<b>1<sup>st</sup> Level</b>	Tamali Roy Phone : +91 87778 33542   Email : <a href="mailto:tamali@primeinfoserv.com">tamali@primeinfoserv.com</a>
<b>2<sup>nd</sup> Level</b>	Shampa Sengupta Phone : +91 99036 87873   Email : <a href="mailto:shampa@primeinfoserv.com">shampa@primeinfoserv.com</a>
<b>3<sup>rd</sup> Level</b>	S Ramakrishnan Phone : +91 98300 17039   Email : <a href="mailto:rama@primeinfoserv.com">rama@primeinfoserv.com</a>

CONFIDENTIAL

# Unlock the Values of NextGen Solution & Services

Accelerate your digital transformation  
Journey with us.

