e mail done
09/10/2025

Haryana Government
Citizen Resources Information Department

हरियाणा सरकार
नागरिक संसाधन सूचना विभाग

No. Admn/315/1SIT/960

To

1. All the Administrative Secretaries to Government of Haryana
2 All the heads of the Department in Haryana
3. All the Divisional Commissioners in Haryana
4. Managing Directors/Chief Administrators/Chief executive Officer of all the Boards, Corporation etc. in Haryana
5 Registrars of all the Universities in Haryana
6. All the Deputy Commissioners in Haryana

Dated Chandigarh, the 09.10.2025

Subject: Approved rates for Security Audit of Web Applications & IT Infrastructure – regarding.

Sir/Madam,

I am directed to address you on the subject citied above and to inform you that the State Government intends to improve / augment the Application Security Audit & IT Infrastructure Security Audit capacity in various Departments/Organizations in the State. Accordingly, CERT-In empanelled organization(s) are shortlisted for the Security Audit of a Website, Mobile Application, API, Server, Laptop/Desktop, Firewall, Mobile Phone and Networking Devices etc. The said auditing organizations, (hereinafter referred to as "Service Provider") would conduct Application & IT Infrastructure Security Audit and provide a valid Cert-In Security Audit certificate on successful completion of Audit (referred to as "Safe-to-Host" Security Audit Certificate), so as to ensure that such Application(s) & IT Infrastructure are safely hosted on production environments.

2. The details of rates approved by the State and accepted by the Service Provider(s) are given below:

Sr.no	Audit Category	Approved Rates (₹) (Inclusive of All Taxes)	Name of Service Providers
Application Security Audit			
Category - 1 (Static Website/Application) (developed in HTML/CMS: WordPress/ Drupal/ Joomla/ DNN etc.)			
1.1	Website Security Audit – Static Website	7,080.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. Ownzap Infosec Private Ltd. iv. InfocusIT Consulting Private Ltd. v. Staqo World Pvt. Ltd vi. BDO India LLP vii. DigiFortex Technologies Pvt. Ltd.
Category - 2 (Dynamic Website/Application) (developed primarily in CMS/ Core with Front End: PHP/.NET/Java, etc.)			

2.1	Web Application Security Audit – Dynamic Pages (1-10) – Small	7,080.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. Ownzap Infosec Private Ltd. iv. InfocusIT Consulting Private Ltd. v. Staqo World Pvt. Ltd vi. BDO India LLP vii. DigiFortex Technologies Pvt. Ltd.
2.2	Web Application Security Audit – Dynamic Pages (11-30) – Medium	8,614.00	i. Dr. CBS Cyber Security Services LLP ii. Ownzap Infosec Private Ltd. iii. InfocusIT Consulting Private Ltd. iv. Staqo World Pvt. Ltd v. BDO India LLP vi. DigiFortex Technologies Pvt. Ltd.
2.3	Web Application Security Audit – Dynamic Pages (31-50) – Enterprise 1	9,440.00	i. Dr. CBS Cyber Security Services LLP ii. Ownzap Infosec Private Ltd. iii. InfocusIT Consulting Private Ltd. iv. Staqo World Pvt. Ltd. v. BDO India LLP vi. DigiFortex Technologies Pvt. Ltd.
2.4	Web Application Security Audit – Dynamic Pages (51-100) – Enterprise 2	11,210.00	i. Dr. CBS Cyber Security Services LLP ii. Ownzap Infosec Private Ltd. iii. InfocusIT Consulting Private Ltd. iv. Staqo World Pvt. Ltd. v. BDO India LLP vi. DigiFortex Technologies Pvt. Ltd.
2.5	Web Application Security Audit – Dynamic Pages (101- 200 Forms) - Enterprise 3	14,750.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. Ownzap Infosec Private Ltd. iv. InfocusIT Consulting Private Ltd. v. Staqo World Pvt. Ltd. vi. BDO India LLP vii. DigiFortex Technologies Pvt. Ltd.
2.6	Web Application Security Audit – Dynamic Pages (>200 Forms) -Enterprise 4	17,700.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. InfocusIT Consulting Private Ltd. iv. Staqo World Pvt. Ltd v. BDO India LLP vi. DigiFortex Technologies Pvt. Ltd.
Category - 3 (iOS/Android Mobile Application)			
3.1	Mobile Application Security Audit dynamic Pages (1-10) – Small	8,496.00	i. Dr. CBS Cyber Security Services LLP ii. Ownzap Infosec Private Ltd. iii. InfocusIT Consulting Private Ltd. iv. Staqo World Pvt. Ltd. v. BDO India LLP vi. DigiFortex Technologies Pvt. Ltd.
3.2	Mobile Application Security Audit dynamic Pages (11-20) – Medium	14,750.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. Ownzap Infosec Private Ltd. iv. InfocusIT Consulting Private Ltd. v. Staqo World Pvt. Ltd.

			vi. BDO India LLP vii. DigiFortex Technologies Pvt. Ltd.
3.3	Mobile Application Security Audit dynamic Pages (21-30) – Enterprise 1	18,000.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. Ownzap Infosec Private Limited iv. InfocusIT Consulting Private Ltd. v. Staqo World Pvt. Ltd. vi. BDO India LLP vii. DigiFortex Technologies Pvt. Ltd.
3.4	Mobile Application Security Audit dynamic Pages (>30) - Enterprise 2	23,500.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. InfocusIT Consulting Private Ltd. iv. Staqo World Pvt. Ltd. v. BDO India LLP vi. DigiFortex Technologies Pvt. Ltd.
Category - 4 (Application Programming Interface (API) including Financial/Banking)			
4.1	API Security Audit: (1-10) methods/ parameters – Small	2,360.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. InfocusIT Consulting Private Ltd. iv. Staqo World Pvt. Ltd. v. BDO India LLP vi. DigiFortex Technologies Pvt. Ltd.
4.2	API Security Audit: (11-30) methods/ parameters – Medium	3,000.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. InfocusIT Consulting Private Ltd. iv. Staqo World Pvt. Ltd. v. BDO India LLP vi. DigiFortex Technologies Pvt. Ltd.
4.3	API Security Audit: (31-60) methods/ parameters - Enterprise 1	4,000.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. InfocusIT Consulting Private Ltd. iv. Staqo World Pvt. Ltd. v. BDO India LLP vi. DigiFortex Technologies Pvt. Ltd.
4.5	API Security Audit: (>60) methods/ parameters - Enterprise 2	4,500.00	i. AKS Information Technology Services Pvt. Ltd. ii. Dr. CBS Cyber Security Services LLP iii. InfocusIT Consulting Private Ltd. iv. Staqo World Pvt. Ltd. v. BDO India LLP vi. DigiFortex Technologies Pvt. Ltd.
IT Infrastructure Security Audit			
Category-5 (Client Systems)			
5.1	Laptop/Desktop Computer/Virtual Machine (as Client System) – Small Category (up to 20 number of Devices/IP)	2,950.00	i. AKS Information Technology Services Pvt. Ltd. ii. InfocusIT Consulting Private Ltd. iii. Staqo World Pvt. Ltd. iv. BDO India LLP v. DigiFortex Technologies Pvt. Ltd.

5.2	Laptop/Desktop Computer/Virtual Machine (as Client System) – Medium Category (from 21 to 50 number of Devices/IP)	4,720.00	i. InfocusIT Consulting Private Ltd. ii. Staqo World Pvt. Ltd. iii. BDO India LLP iv. DigiFortex Technologies Pvt. Ltd.
5.3	Laptop/Desktop Computer/Virtual Machine (as Client System) – Enterprise Category (more than 51 number of Devices/IP)	5,900.00	i. InfocusIT Consulting Private Ltd. ii. Staqo World Pvt. Ltd. iii. BDO India LLP iv. DigiFortex Technologies Pvt. Ltd.
5.4	Printer/Scanner	354.00	i. Ownzap Infosec Private Ltd. ii. InfocusIT Consulting Private Ltd. iii. Staqo World Pvt. Ltd. iv. BDO India LLP v. DigiFortex Technologies Pvt. Ltd.
Category-6 (Server/Workstation Systems)			
6.1	Server/WorkStation/Virtual Machine (as Host System)	560.50	i. Ownzap Infosec Private Ltd. ii. InfocusIT Consulting Private Ltd. iii. Staqo World Pvt. Ltd. iv. BDO India LLP v. DigiFortex Technologies Pvt. Ltd.
Category-7 (Networking Devices)			
7.1	L2 Switch/Internet Lease Line Router	442.50	i. Ownzap Infosec Private Ltd. ii. InfocusIT Consulting Private Ltd. iii. Staqo World Pvt. Ltd. iv. BDO India LLP v. DigiFortex Technologies Pvt. Ltd.
7.2	L3 Switch/Video Conferencing Bridge (MCU)	678.50	i. Ownzap Infosec Private Ltd. ii. InfocusIT Consulting Private Ltd. iii. Staqo World Pvt. Ltd. iv. BDO India LLP v. DigiFortex Technologies Pvt. Ltd.
7.3	Wi-Fi Access Point/Router	442.50	i. Ownzap Infosec Private Limited ii. InfocusIT Consulting Private Limited iii. Staqo World Pvt. Ltd iv. BDO India LLP v. DigiFortex Technologies Pvt. Ltd.
Category-8 (Security Device/System)			
8.1	DDoS/Load Balancer/APT	590.00	i. Ownzap Infosec Private Ltd. ii. InfocusIT Consulting Private Ltd. iii. Staqo World Pvt. Ltd. iv. BDO India LLP v. DigiFortex Technologies Pvt. Ltd.
8.2	Firewall/UTM/WAF/IPS/NGFW	590.00	i. Ownzap Infosec Private Ltd. ii. InfocusIT Consulting Private Ltd. iii. Staqo World Pvt. Ltd. iv. BDO India LLP v. DigiFortex Technologies Pvt. Ltd.
Category-9 (Mobile Device)			
9.1	Mobile Phone (Android/iOS) / Tablet (Android/iOS)	4,720.00	i. Ownzap Infosec Private Ltd. ii. InfocusIT Consulting Private Ltd. iii. Staqo World Pvt. Ltd. iv. BDO India LLP v. DigiFortex Technologies Pvt. Ltd.

Note:

(i) Each Security Audit Work Order of IT Infrastructure (for Category 5 to 9) may be considered for a value of ₹20,000/- to ensure financial viability with Service Provider.

(ii) As per letter no. Admn/315/1SIT/23 dated 07.01.2025, the existing approved rates remain valid till 17 November 2025. Organizations are advised to refer to these rates (where lower than current ones) before issuing work orders up to the said date.

3. The contact details of above CERT-In empanelled organization/ Service Provider(s) are:

Sr. No	Service Provider Name	Address	Contact Person/Phone no.	Email
1	AKS Information Technology Services Pvt. Ltd	B-21, Sector-59, Noida-201309, UP	Sh. Vivek Verma-9899357568 Sh. Prince Bajaj 9760135533	vivek.verma@aksitservices.co.in prince.bajaj@aksitservices.co.in
2	Dr. CBS Cyber Security Services LLP	113, East Suraj Nagar Civil Lines, Jaipur-302006, Rajasthan	Dr. CB Sharma IPS R - 9828877777 Sh. Satyendra Singh-9783380412 01412229475	contact@drcbscyber.com
3	Ownzap Infosec Pvt. Ltd.	1st Floor, 15, Karyagrah, Savina Main Road Udaipur, Rajasthan, India, 313001	Sh. Puneet Matta 9875770345 Sh. Punith Kumar MP 9353549700	puneet@ownzapinfosec.co.in kumar@ownzapinfosec.co.in
4	INFOCUS IT Consulting Pvt. Ltd.	A-19, Yadav Park, Rohtak Road, Behind Bank of Baroda, West Delhi-110041, India	Sh. Jagbir Singh 8800827932 Sh. Rupal Goley 8178210903	jagbir@infocus-it.com support@infocus-it.com
5	Staqo World Pvt. Ltd.	603 Ashadeep, 9 Hailey Road, NEW Delhi, 110001	Sh. Jaspreet Singh, 9310600697 Sh. Neelesh Gaur 9599185838 Smt. Kanika 9650217931 0120 468 6440	jaspreet.singh@staqo.com contactus@staqo.com neelesh.gaur@staqo.com kanika@staqo.com
6	BDO India LLP	Windsor IT Park, Plot No. A-1, Floor 2, Tower B, Sector 125 NOIDA 201301	Sh. Anurag Srivastava - 9717004947 Sh. Priyanka Sikdar - 8260304302 0120-4557532	anuragsrivastava@bdo.in priyankasikdar@bdo.in sunakshirattan@bdo.in randeepsingh@bdo.in
7	DigiFortex Technologies Pvt. Ltd.	Unit #2CW, Neil Towers 2nd floor, Plot No 117 & 118, Road No 3, Vijayanagar, EPIP Phase I, Whitefield, Bangalore 560066	Sh. Vijay Kumar 9448353194	vijay@digifortex.com sanya.shree@digifortex.com katyayani.basak@digifortex.com pratidhee.palak@digifortex.com

Any Department/Organization/Board/Corporation/University etc. in the State (referred to as 'Indenting Agency') may place the work order for any service referred above, on the approved rates with the respective 'Service Provider' based on the category and size of the Application/number of Systems with a copy to Information Security Management Office (ISMO), CRID Haryana, First Floor, SCO 109-110, Sector 17B, Chandigarh, email id: support.desk@haryanaismo.gov.in, Contact No: 0172-2709250.

Further, the General Terms & Conditions are enclosed at Schedule 'A'; the Objectives & Audit Process is provided at Schedule 'B'; and the Roles & Responsibilities of the Service Provider, Indenting Agency and ISMO are detailed at Schedule 'C'.

For any further assistance regarding security audit of Applications & IT Infrastructure please contact with Sh. Munish Chandan, Addl. CITO cum Dy. CISO at email munishchandan.crid@hry.gov.in and Sh. Amit Beniwal, Sr. ISQA at email amit.beniwal@haryanaismo.gov.in .

Director Admin,
for Additional Chief Secretary to Govt. Haryana
Citizen Resources Information Department

Schedule 'A'

General Terms & Conditions:

(a) The empanelment/approved rates shall be valid for a period of 2 years (from 01 Oct. 2025 to 30 September 2027). CRID reserves the right to terminate/curtail the approved rates at any time owing to deficiency of service, substandard quality of manpower used and work done, inordinate delays, breach of agreement, etc. or even without assigning any reason.

(b) The Service Provider shall not be allowed to transfer, assign, pledge or subcontract any activity to another agency.

(c) As the basis of the empanelment is CERT-In empanelment of the Service Provider, as such if the CERT-In empanelment is expired/ cancelled prior to the 2 years, the empanelment shall cease to exist.

(d) In case, if any document(s) furnished by Service Provider are found to be false/ forged at any stage, it would be deemed to be a breach of terms making the Service Provider liable for legal action besides termination from the empanelment/ approved rates.

(e) The Service Provider shall maintain all statutory registers under Law, and shall produce the same on demand, to the concerned authority of Govt. of Haryana / CRID or any other authority under Law.

(f) Special Secretary (IT), CRID reserves the right to withdraw / relax any of the General terms and conditions mentioned above so as to overcome a problem encountered.

(g) CRID reserves the right to examine the performance of the Service Provider or work carried out at any stage and the Indenting Agency and Service Provider would be required to support the same.

(h) Confidentiality: Except or otherwise permitted by the agreement, the Service Provider may not disclose to third parties the content of this agreement or any information provided by or on behalf of the government that ought reasonably to be treated as confidential and or proprietary. Service Provider may however, disclose such confidential information to the extent that it:

   i. Is or become public other than through a breach of agreement
   ii. Is subsequently received by the receiving party from a third party who, to the receiving party's knowledge, owes no obligation of confidentiality to the disclosing party with respect to that information.
   iii. Was known to the receiving party at the time of disclosure or is created independently.
   iv. Is disclosed as necessary to enforce the receiving party's right under this agreement, or
   v. Must be disclosed under applicable law, legal process or professional regulations.
   vi. These obligations shall be valid for a period applicable under provisions of the IT Act 2000.

(i) Non-Disclosure Agreement (NDA) must be signed by the Service Provider with the Indenting Agency before commencement of the security audit & must be legally enforceable. CERT-In 'Model NON-Disclosure Agreement' is available at Cert-In Web Site https://cert-in.org.in/ under tab 'Cyber Security Assurance' -> 'Empanelment by Cert-In' for reference.

(j) The copy of the work order and 'Safe to Host' Certificate shall be shared with ISMO/CRID at support.desk@haryanaismo.gov.in by the 'Indenting Agency' before initiating any audit for information.

Payment terms:

(a) Payments towards Security Audits would be released directly by Indenting Agency to the respective Service Provider.
(b) The selected 'Service Provider' shall deposit 10% Bank Guarantee (BG) of the work order with the Indenting Agency before executing of work where total work order value more than ₹ 1 Lac.
(c) The Indenting Agency may release 50% of the payment based on the Audit report and support extended to development team for removal of vulnerabilities. The remaining 50% may be released after completion of Audit exercise and submission of Safe to Host Certificate.
(d) The BG can be forfeited by the Indenting Agency under rules, in case the 'Service Provider' does not perform or compete the assigned work as per requirements of the issued Work order.

Schedule 'B'

Objective:

The selected vendor(s) (henceforth referred to as "Service Provider(s)" would provide "Safe-to-Host" Security Audit Certificates for the Applications & IT Infrastructure, in conformance with the directions & guids issued Cert-In, Government and regulatory bodies.

The overall objective of the work is to review the security controls / vulnerability assessments & Penetration Testing of Applications and IT Infrastructure in order to meet the confidentiality, integrity and availability requirements of the organizations. Further, in order to promote a seamless, effective, and efficient auditing process, the 'Comprehensive Cyber Security Audit Policy Guidelines' available at URL: https://cert-in.org.in/PDF/Comprehensive_Cyber_Security_Audit_Policy_Guidelines.pdf provide a thorough guidance for both 'Indenting Agency' and the 'Service Provider' involved in security audits.

Audit Process:

(a) The Service Provider(s) along with their approved rates for various categories shall be published by ISMO, CRID Haryana. The Departments/ Boards/ Corporations/ Districts (Indenting Agencies) would contact the Service Provider(s) and would allot the work based on the requirements on the approved rates.

(b) The Service Provider(s) would use their own vulnerability scanning tools (Vulnerability Assessment / Penetration Testing), for conducting the security audit of the Applications & other IT Infrastructure and facilitate the Indenting Department/Agencies to carry out bug fixing so that the Cert-In Security Audit 'Safe to Host' certificate is attained for the required Application & IT Infrastructure.

(c) The assessment should be done completely ethically and the Service Provider(s) should not reveal the information arising from the Security Audit to any other party except ISMO, CRID Haryana/Indenting Agencies/Cert-In. For the purpose, the service provider will sign a 'Non-Disclosure Agreement'. Any breach in this regard shall lead to penalizations under IT Act 2000 and its amendments.

(d) In order to improve the security of the Applications / IT Infrastructure, the security audit should be in compliance with Cert-In directions & guidelines, Government and regulatory bodies.

(e) Standards/references for security audit should not be limited to the lists such as top 10, top 25. The Security Audit should include discovery of all known vulnerabilities based on comprehensive framework and standards like ISO/IEC, Cyber Security Audit Baseline requirements, OWASP Web Security Testing Guide, Application security verification standards along with applicable regulatory framework and directions issued by CERT-In and other agencies.

(f) Minimum two different tools shall be used for the security audit and it should include evaluation whether the code/device configuration can be manipulated by attacker to communicate sensitive data out of the organization, and check the different validations so as to ensure the level of IT security desired.

(g) The Service Provider is expected to assist the Indenting Organization, suggest remedial solutions or provide recommendations against the vulnerabilities, threats or risks so as to help into mitigation of the same.

(h) 'Safe-to-host' certificate will be issued in compliance of Cert-In Security Audit Guidelines having validity of 1 Year and without any conditions such as risk ownership or non-conformity to Medium & High/Critical Vulnerabilities for Application(s) & IT Infrastructure under Security Audit.

(i) In order to perform the Security Audit successfully, and enable the Applications & IT Infrastructure under audit achieve 'Safe to Host' Certificate, any activity required such as vulnerability assessment/configuration review needs to be performed. Optionally, penetration testing, code review, if needed on a case to case basis may be performed for which a rate discovery shall be made separately by the respective Department in consultation with ISMO.

(j) For IT Infrastructure Security Audits, the indenting Agency may opt limited or selective systems/devices based on sampling/random and would be part of scope of assignment.

(k) Payments towards Security Audits would be released directly by indenting departments to the Service Provider(s).

(l) The validity of the empanelment shall exist only until the company is empanelled with the Cert-In or the duration of empanelment under the scope of this RFP (whichever is earlier).

(m) The Service Provider is responsible for documentation and reporting requirements during the audit for each Application/IT Infrastructure Audit, such as (but not limited to):

(i) Work Order Reference
(ii) Audit Plan/Actions taken
(iii) Duration of Audit/No of iterations etc.
(iv) Additional mandatory or voluntary standards or regulations applicable/ applied for conducting audit.
(v) Summary of audit findings including identification tests, tools used, and results of tests performed.
(vi) Analysis of vulnerabilities and issues of concern.
(vii) Recommendations for action.

(n) The Service Provider is expected to perform audit in multiple rounds of iterations (if required), and share the Audit reports to the Indenting Agency (Application/IT asset owner), who in turn shall be responsible for resolution of the issues in a time bound manner.

(o) ISMO, CRID Haryana may desire various reports from the Service Provider as indicated above and the Service Provider would share the same reports as desired within desired timelines. The Service Provider is expected to provide an MIS / Dashboard (preferably) with access to ISMO, CRID Haryana, which would help in sharing the data related to the audits performed, their complexity, iteration details, cost etc. periodically and or on need basis.

(p) During the process, any resources to be deployed from Service Provider, such as employees, software, hardware, equipment used if any for performance of the service would be the responsibility of Service Provider only. The Indenting agency or ISMO, CRID Haryana would not be responsible or liable for any of these resources, such as license expiry, hardware failure, or health issues, leaves etc. and under all such cases, the Service Provider would be responsible for providing the needed replacements in time, so that there is no delay in performance of audit due to these eventualities.

(q) Any transportation, boarding and lodging facility, if required for the performance of the security audit activities would be borne by the Service Provider.

(r) This Indenting Agency/ISMO, CRID Haryana or any other State department/ agency, shall not be liable for any loss, damage, theft, burglary or robbery of any personal belongings, equipment or vehicles of the personnel of the Service Provider.

(s) The Service Provider(s) Single Point of Contact (SPOC) person shall be contactable at all times and message sent by phone/email/Special Messenger/Fast Messaging Apps from this Department to the agency / selected Service Provider shall be acknowledged immediately on receipt on the same day.

(t) The service charges/rates charged by the Service Provider shall be strictly as per Approved Rates for the period of contract (and extended contract period as applicable) and no additional amount shall be charged.

(u) Considering the scope of work and requirements of Intending Department's/Organizations; Security Audit of Web Applications/API/Mobile Apps may be carried out offsite/remotely. However, Security Audit of IT Infra/Systems has to be carried out Onsite.

(v) Security Audit based on sample basis is not allowed; All IT Infra/Systems should be audited as per the scope of work.

Tentative Timelines (in Max Working Days):

SL	Item	Category – Small	Category - Medium	Category - Enterprise
1.	Release of WO	T0	T0	T0
2.	1st Audit Report	T1=T0+3	T1=T0+7	T1=T0+9
3.	Follow-up with Indenting Agency & Bug Fixing (1st Round)	T2= T1+3	T2= T1+7	T2= T1+9
4.	2nd Audit report	T3=T2+2	T3=T2+3	T3=T2+4
5.	Follow-up with Indenting Agency & Bug Fixing (2nd Round)	T4= T3+2	T4= T3+3	T4= T3+5

6.	Release of Application Audit Certificate ('Safe-to-host' certificate)	T5=T4+1	T5=T4+3	T5=T4+3

Note:

a) For IT Infrastructure Security Audits across multiple locations in Haryana, timelines shall be mutually agreed between the Service Provider and the Indenting Agency/Department.

b) The Service Provider(s) has to abide to the terms & conditions as per Tender ID: 2025_HRY_436887 and instructions issued by ISMO, CRID Haryana from time to time for smooth functioning.

Schedule 'C'

Roles & Responsibilities of Service Provider(s)

a) Service Provider will nominate a person in the capacity of a Project Manager/ SPOC, who will serve as the single point of contact for the Indenting Agency and attend all meetings related to the security audit project under the scope of the Work Order with the Indenting Agency and / or ISMO, CRID Haryana.
b) Follow latest Guidelines for CERT-In Empanelled Information Security Auditing Organizations from CERT-In as applicable from time to time.
c) Plan & execute the security audits through a suitably qualified technical team/auditors always completing the Scope of Work as mentioned in the Work Order entered upon with the Indenting Agency.
d) The Service Provider is expected to carry out an assessment of the vulnerabilities, threats and risks that may exist in the respective Web Application/ IT Asset through industry standard methodologies, best practices for security testing ensuring that the audit process is thorough, unbiased and meets established standards of quality.
e) As part of security audit, the following standards and frameworks has to be followed, but not limited to:
    i Discovery of all known vulnerabilities based on the comprehensive standards/frameworks like ISO/IEC
    ii Cyber Security Audit Baseline Requirements
    iii Security, Open Source Security Testing Methodology Manual (OSSTMM3)
    iv OWASP Web Security Testing Guide for web application security testing
    v OWASP Application Security Verification Standard (ASVS) for establishing and verifying application security controls
    vi OWASP Mobile Security Testing Guide (MSTG) for Mobile App Audits and
    vii Directions & Guidelines issued from time to time by agencies such as Cert-In, Government and regulatory bodies.
f) The Service Provider is responsible for documentation and reporting requirements during the audit, such as:
    i Terms of reference (as agreed between the Indenting Agency and Service Provider), including the standard for audit, if any.
    ii Audit Plan with timelines
    iii Explicit reference to key auditee organization documents including policy and procedure documents, if any.
    iv Additional mandatory or voluntary standards or regulations applicable to the auditee.
    v Summary of audit findings including identification tests, tools used, and results of tests performed.
    vi Analysis of vulnerabilities and issues of concern.
    vii Recommendations for action.
    viii Closure Report
g) Submit periodic reports and support project reviews as per the scope of Work Order or any other as required by ISMO/ CRID or Indenting Agency.

h) To complete the Scope of work preferably in the tentative timelines prescribed in the Work Order.
i) On successful completion of security audit of a Website/application/API/Mobile App/IT Systems the Service Provider will provide a valid Security Audit Certificate ("safe-to-host") as per CERT-In guidelines & directions.

Roles & Responsibilities of Indenting Department/Agency:

a) Release Work order and Payments following the terms as mentioned and follow rates as agreed under the scope of this empanelment/approved rates. The copy of the Work Order has to be shared with ISMO, CRID Haryana.
b) Appoint Nodal officer for coordination with empanelled agency and to fix the responsibilities of development teams for timely audit exercise.
c) The Indenting Department/Agency shall facilitate timely vulnerability patching as per the Audit reports submitted by Service Provider for obtaining the 'Safe to host' certificate within timelines.
d) To carry out project tasks which fall under the Departmental responsibility, within reasonable time limits, particularly in matters related to reviews, approvals, acceptance, etc.
e) Provide the required timely access to technical personnel, clarifications, and decisions and to resolve any issues as may be necessary for the respective Service Provider to carry out their obligations under the scope of the work order.
f) Provide dummy data, staging environment with the hosted platform for audit as desired for the successful conduct of audit activities.

Roles & Responsibilities of ISMO team:

a) ISMO will publish the approved rates on its web site. The same would be visible to everyone, who accesses the website, but applicable only to Service Providers.
b) ISMO will evaluate the audit quality, performance of Service Providers.
c) ISMO will establish a central repository for completed security audit certificates.
d) ISMO can ask for detailed Security Audit report from Indenting Agency / Service Provider to understand the vulnerabilities/threat landscape at State Level.