Request for proposal (RFP) for Auditing services regarding the assessment of Cybersecurity Compliance for Bhutan Telecom's Mobile Network, IT infrastructure, and Data Centre Services.

TABLE OF CONTENTS

BACKGROUND

Bhutan Telecom Limited (BT) is the leading provider of telecommunications and Internet services in the Kingdom of Bhutan. Besides fixed line telephony, BT provides GSM Mobile Services and Internet Services. It is the leading provider of Mobile services, Internet services in the country, and the only fixed line telephony service provider in the country along with colocation services of the Data Centre in Phuentsholing.

Bhutan Telecom Limited is accepting proposals in response to this Request for Proposal (this RFP or this "Request for Proposal" in order to find a qualified firms to provide Cyber Security Compliance Assessment Services and Support and to be delivered and installed at our Centre with detailed Cyber Security Compliances as per the scope in RFP but not limited to.

The objective of this RFP is to locate a source that will provide the best overall value to 'BT'. While price is a significant factor, other criteria will form the basis of our award decision, as more fully described in the Evaluation Factors section of this RFP below.

The Bidder (Single Party/Joint Party) should have a back-to-back arrangement as applicable to ensure a seamless communication and support as required through the RFP process for timely responses. The Bidder should provide a Single Point of Contact along with the escalation matrix mentioning the contact person's name, number and designation in the company for all or any technical and commercial queries through the process.

OBJECTIVES

Identify & design a robust Cyber–Security Framework for the organization and enable the same by Implementing Cyber–Security Assurance Compliance & IT Security Resilience Assessment Exercise as Controls for Effective Cyber Resilience. This is to provide a framework for managing and improving the security of an organization's information assets, securing business continuity, and reducing the risks of business disruptions due to cybersecurity incidents. In addition, the audited cybersecurity compliance assessment report is to help BT comply with legal and regulatory requirements related to information security, and improve their resilience against cyber threats and data breaches.

DUE DILIGENCE

The Bidder is expected to examine all instructions, forms, terms and specifications in this RFP and study the Bid Document carefully. Bid shall be deemed to have been submitted after careful study and examination of this RFP with full understanding of its implications. Each Bidder should, at its own costs without any right to claim reimbursement, conduct its own investigations, analysis and should check the accuracy, reliability and completeness of the information in this RFP and wherever felt necessary obtain independent advice or seek clarity. The Bid should be precise, complete and in the format as per the requirement of this RFP. Failure to furnish all information required by this RFP or submission of a Bid not responsive to this RFP in each and every respect shall be at the Bidder's own risk and may result in rejection of the Bid and for which BT shall not be held responsible. Any decision taken by BT, as to completeness of the Bid and/or rejection of any/all Bid(s) shall be final, conclusive and binding upon the Bidder(s) and shall not be questioned/challenged by the Bidder(s).

The Bidder shall solely bear all expenses whatsoever associated with or incidental to the preparation and submission of its Bid and the BT shall in no case be held responsible or liable for such expenses, regardless of the conduct or outcome of the bidding process including but not limited to cancellation/abandonment/annulment of the bidding process.

CONFIDENTIALITY

All documents, information and reports relating to the assignment would be handled and kept strictly confidential and not shared/published/supplied or disseminated in any manner, by the Bidder and appropriate NDA/Confidentiality Statement will be signed by the Bidder before start of the engagement

SCOPE OF WORK

The followings are the overall terms of reference to assess the overall scope of work

Domain	Objective
1. Cybersecurity & Data Privacy Governance (GOV)	Implement a documented, risk-based cybersecurity and data privacy program that supports business objectives while meeting applicable statutory, regulatory, and contractual requirements
2. Asset Management (AST)	Ensure the secure use of all technology assets, both physical and virtual, from purchase through disposition.
3. Business Continuity & Disaster Recovery (BCD)	Through well-documented and practised processes, sustain business-critical functions while successfully responding to and recovering from incidents
4. Capacity & Performance Planning (CAP)	Manage and oversee the current and future capacities and performance of the technology assets within the organisation
5. Change Management (CHG)	Maintain a sustainable and ongoing change management process that includes both the technology stakeholders as well as business stakeholders in order to ensure that only authorised changes are made to technology systems and procedures
6. Compliance (CPL)	Monitor and supervise the implementation of cybersecurity and data privacy controls to make sure that appropriate evidence is available to demonstrate that due care and due diligence had been taken in order to meet compliance with applicable statutory, regulatory and contractual obligations.
7. Configuration Management (CFG)	The secure configuration of systems, applications and services should be enforced in accordance with industry-

Domain	Objective
	recognized secure practices and vendor-recommended configurations
8. Continuous Monitoring (MON)	Ensure situational awareness of cybersecurity-related events by collecting and analysing event logs from systems, applications, and services in order to maintain situational awareness of cybersecurity-related events
9. Cryptographic Protections (CRY)	Make use of appropriate cryptographic solutions and industry-recognized key management practices in order to ensure the confidentiality and integrity of sensitive/regulated data at rest and in transit
10. Data Classification & Handling (DCH)	Ensure that a standardized data classification methodology is in place so that it is possible to objectively determine the sensitivity and criticality of all the data and technology assets so that proper handling and disposal requirements are met
11. Embedded Technology (EMB)	As a result of the potential damages posed by malicious use of embedded technology, it is important to conduct additional scrutiny to reduce the risks associated with embedded technology
12. Endpoint Security (END)	Make sure that endpoint devices are hardened so that they are protected against reasonable threats to them and the data they store, transmit and process.
13. Human Resources Security (HRS)	Develop a cybersecurity and privacy-minded workforce by implementing sound hiring practices and performing on-going personnel management to ensure a safe and secure workplace
14. Identification & Authentication (IAC)	Through a documented and standardised Identity and Access Management (IAM) capability, the concept of 'least privilege' is enforced across all systems, applications and services for individual, group and service accounts in a consistent manner.
15. Incident Response (IRO)	Establish a viable incident response capability that trains personnel in how to recognize suspicious activity and how to report it in order for trained incident responders to take the appropriate steps to respond to incidents in accordance with a documented Incident Response Plan (IRP)

Domain	Objective
16. Information Assurance (IAO)	Assess the existence and functionality of appropriate cybersecurity and privacy controls prior to deploying a system, application, or service in a production environment
17. Maintenance (MNT)	Provide proactive maintenance of technology assets, including those that are hosted or supported by third parties, in accordance with current vendor recommendations
18. Mobile Device Management (MDM)	Implement measures to limit the attack surface and potential data exposure resulting from mobile device usage by restricting mobile device connectivity to critical infrastructure and sensitive/regulated data.
19. Network Security (NET)	Establish a defence-in-depth methodology that enforces the concept of "least functionality" by restricting network access to systems, applications, and services
20. Physical & Environmental Security (PES)	Ensure physical environments are protected from theft and damage by layers of physical security and environmental controls
21. Data Privacy (PRI)	Integrate appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services in accordance with industry-recognized data privacy principles
22. Project & Resource Management (PRM)	Ensure that cybersecurity is integrated into project management practices in order to deliver resilient and secure solutions
23. Risk Management (RSK)	Establish a risk threshold for organisation to ensure that risk decisions adhere to industry-recognized risk management principles
24. Secure Engineering & Architecture (SEA)	Develop secure, resilient systems, applications, and services based on industry-recognized engineering and architecture principles
25. Security Operations (OPS)	Implement cybersecurity and privacy operations to meet the business needs of the organisation by providing secure systems, applications, and services

Domain	Objective
26. Security Awareness & Training (SAT)	Promote cybersecurity awareness and privacy awareness among employees by educating them on evolving threats, compliance obligations, and secure workplace practices
27. Technology Development & Acquisition (TDA)	To reduce potential impact of undetected or unaddressed vulnerabilities and design weaknesses, develop and test systems, applications or services according to a Secure Software Development Framework
28. Third-Party Management (TPM)	Ensure that only trustworthy third parties are used for delivering products and/or services.
29. Threat Management (THR)	Develop a proactive approach to identifying and assessing technology-related risks and how they affect assets and business processes
30. Vulnerability, Patch Management (VPM) and penetration testing	Improve the security and resilience of systems, applications and services against evolving and sophisticated attack vectors by leveraging industry-recognized Attack Surface Management (ASM) practices
31. Web Security (WEB)	Utilise secure configuration management practices and monitor anomalous activity to ensure Internet-facing technologies are secure and resilient

TECHNICAL OBJECTIVE AND KEY DELIVERABLES

Based on the above areas of objectives the following key components are to be captured neatly and delivered as part of the exercise mentioned in this RFP. BT has identified three parts to this project: and anticipates that the nature of the work will involve, but not limited to, the following:

Components	Description
Project Management	• Develop project charter. • Develop project plan & Execution Methodologies. • Project control and progress reporting. • Assist BT in determining & finalizing the scope covering application and IT and telecom network services with BT premises by conducting a detailed study to evaluate the Cyber Security Compliances and prepare the plan.

	• Study of current security structure, security architecture & processes, roles, skills set, asset registry and security culture. • Identify & document all information assets and identify their criticality & sensitivity to business operations and develop classification mechanisms. • Develop a detailed implementation plan.
Part 1: Detailed Scope for Assessment and Consulting	• Assist BT in determining & finalizing the scope covering application and IT and Telecom network services with BT premises by conducting a detailed study to evaluate the Cyber Security Compliances and prepare the plan. • Study of current security structure, security architecture & processes, roles, skills set, asset registry and security culture. • Identify & document all information assets and identify their criticality & sensitivity to business operations and develop classification mechanisms. • Develop a detailed implementation plan.

Part 2: Penetration tests and Vulnerability Scan and assessment for all applicable IT and Telecom critical assets as documented in Scope Document.	• Conducting Risk assessment as per scope
	• Preparing a Risk mitigation plan
	• Conducting vulnerability scan and penetration tests as per the Scope document.
	• Reviewing the security and antivirus policies.
	• Audit all the access controls facing customers/clients and internet
	• Evaluate the effectiveness of intrusion detection and prevention systems.
	• To implement a security control effectiveness measurement and tracking process that would enable the management to review the security effectiveness and take corrective/preventive actions.
	• IT and Telecom Network Vulnerability Assessment and Risk Assessment including thread modelling of:
	  ○ Network Infrastructure
	  ○ Network Applications
	  ▪ Audit must be carried out on critical Software Applications and Packages that are exposed to the Internet in telecom networks and ISP infrastructure.

	● Penetration Testing
	  o Network Infrastructure
	  o Network Protocol/Interfaces (SS7, Diameter, GTP)
	● Network Security Configuration review based on the vulnerability assessment.
	● The audit will evaluate key security aspects, including encryption standards like AES and RSA, compliance with data protection regulations and adherence to internal privacy policies. It will also assess authentication methods like multi-factor and biometric authentication, as well as access control through RBAC. Continuous monitoring, incident response for various cyber threats like DDoS and phishing attacks, and proactive vendor risk management, employee training, and patch management will also be scrutinised during the audit.
	● All internal & external - Web Applications, Telecom Applications, Mobile Applications, Software Security Configuration Review of all Third-Party Software / Applications.
	● The 'best practices' shall be drawn as per requirements given in global standards like ISO 27001, NIST, ITU-T x.805 security architecture,3GPP, GSMA security guidelines, ENISA, COBIT, OWASP and other such frameworks and to the extent applicable to telecom operators.

Part 3: Final Report	● Shall provide an action plan to close the technical noncompliance vulnerabilities identified during risk assessment exercise. ● Recommend an effective and sustainable security awareness program that helps the organisation to impart security awareness among the users and measure awareness effectiveness. ● Define and prepare a corporate level information Communication security policy that is in line with business objectives, and that will become the baseline for planning the Information Security investments. ● Develop metrics to determine compliance and security program effectiveness ● Assist BT in establishing, implementing, and operating, monitoring, and reviewing, maintaining, and improving, the security practice. o Identification of vulnerabilities,

	○ Evaluation of potential risks, ○ Prioritization of risks, ○ Incident response plans, ○ Mitigation measures and recommendations ● Preparing an audit schedule. ● Assisting in the overall implementation, operation monitoring and improvement activities for the security practice. ● Proposing for any required industry certification for the future as needed.

HIGH LEVEL ASSET LISTING

Description	Quantity	Make(OEM)
Databases	10	propreity database,Oracle, Ericsson,honeywell
Router/Switches	55	CISCO and JUNOS
Servers	89	Dell, HP, Supermicro, Ericsson
Servers Related Telecom Services	32	Ganeti, VmWare, Enterprise Building Intregrator, Propritery data storage, Load Balancer.
Total Numbers of Application	76	Bind9, Zimbra, cPanel, DirectAdmin, Quagga,Oracle,ErpNext, Laravel, proprietary softwares
Total Number of OS	114	CentOS, Ubuntu, Windows, linux server 7.3(Maipo),SUSE Linux Enterprise 12, Oracle Solaris,Ericssion,Debain, Oracle, SunOS,EU5_Linux AOM, Linux, iLO, SUSE Linux, ExtremeXOS, Junos, RedHat
Total Number of approx. Staff	600	
MSC or Packet Gateways	6	Erission, Huawei, Allot
Firewall	5	CISCO
Media Gateway	2	VoLTE

LOCATION OF WORK

The audit and Assessment will be conducted on site at Bhutan Telecom Limited Campus in Thimphu (Mobile and ICT Infrastructure) and in Phuentsholing (Data Centre Services).

DOCUMENTATION

All documentation required for as mentioned in the final report section, importantly baseline security policy documents need to be completed & submitted to the BTL by the Service Provider.

SINGLE POINT OF CONTACT

The shortlisted Bidder shall appoint a single point of contact (Project Manager) with whom the BT will deal for any activity pertaining to the requirements of this RFP.

BID EVALUATION CRITERIA & SUBMISSION GUIDELINES:

To meet the requirements, as spelt out in this Bid Document, the selected Bidder must have the requisite experience and expertise in providing services in the field of information and communication technology and telecom operation, the technical know-how, and the financial ability that would be required to successfully set-up the required infrastructure and provide the services sought by BT.

The Bidder shall submit their offers strictly in accordance with the terms and conditions of the Bid Document. Any Bid, which stipulates conditions contrary to the terms and conditions given in the Bid Document, is liable for rejection. Any decision of BT in this regard shall be final, conclusive and binding on the Vendor.

1. The Bidders shall be short listed for commercial evaluation only after the evaluation of their Technical Bids. To pass the technical evaluation, a minimum score of 80% must be attained

2. BTL reserves the right to modify/amend the evaluation process at any time/at any stage during the Bid process, without assigning any reason, whatsoever, and without any requirement of intimating the Bidders of any such change. Any time during the process of evaluation BT may seek specific clarifications from any or all Bidders.

3. The Bidder shall produce a self-declaration that.

    (i) They are duly authorized persons to submit this undertaking.

    (ii) They have read and understood the RFP and have conveyed their absolute and unconditional acceptance to the RFP.

    (iii) They do not have any business relationship with BT including its directors and officers which may result in any conflict of interest between us and BT. They shall on occurrence of any such event immediately inform the concerned authorities of the same.

    (iv) They have submitted a Bid in compliance with the specific requirements as mentioned in this RFP.

    (v) They have provided with all necessary information and details as required by BT and shall provide with such additional information may be required by BT, from time to time.

(vi) Neither they nor any of their employee/director has been barred from providing the Services nor are they in negative list/blacklisted by any public sector BT statutory or regulatory or investigative agencies in Bhutan, India OR Asia or abroad in the last 5 years.

(vii) There is no vigilance and/or court cases pending against them/company and no inquiry or investigation pending against them from any statutory regulatory and/or investigation agency.

(viii) All the information furnished in and as per the document submitted is true and accurate and nothing has been concealed or tampered with. They have gone through all the conditions of Bid and are aware that they would be liable to any punitive action in case of furnishing false information/documents.

(ix) They also undertake that, they were/are never involved in any legal case that may affect the solvency/existence of their organization or in any other way that may affect capability to provide/continue the services to us as they will further certified that they have not modified or deleted any text/matter in the RFP.

Note: Bidder must comply with all the above-mentioned criteria as specified above and more elaborately. Non-compliance of any of the criteria can entail rejection of the offer.

Photocopies of relevant documents/certificates should be submitted as proof as applicable in support of the claims made for each of the above-mentioned criteria and as and when BT decides, originals/certified copies should be shown for verification purpose.

BT reserves the right to verify/evaluate the claims made by the Bidder independently. Any deliberate misrepresentation will entail rejection of the offer ab-initio.

The following submission guidelines & requirements apply to this RFP:

1. First and foremost, only qualified individuals, partnerships, or firms with prior experience on projects such as this should submit proposals in response to this RFP.
2. Proposals must be signed by a representative that is authorized to commit bidder's company.
3. If you have a standard set of terms and conditions, please submit them with your proposal. All terms and conditions will be subject to negotiation.
4. Proposals must be received prior to submission dateline to be considered.
5. Proposals must remain valid for a period of 180 days.

VENDOR QUALIFICATION CRITERIA

1. A minimum of three years of experience in Cyber Security and Data Protection Consultancy.
2. Conducted at least three similar consultancy assignments for Telecom operators.

3. The Vendor should have got minimum three successful Cyber Security Audit Assessments/ISO 27001 implementations. Minimum three such project completion certificates shall be required to be submitted from different client organisations with client references.
4. Vendor company should be ISO 9001, ISO 27001 certified OR any other equivalent certifications. Minimum three such project completion certificates shall be required to be submitted from different client organisations with client references.
5. Last 3 financial years' Turnover of bidder should be higher than twenty million (INR).
6. Bidders should have a minimum of three CISA/CISSP/ISO 27001 Lead Auditor certified auditors in the team - three Certified Professional Profiles need to be submitted with their active certification details. List of all various tools and software required for performing security testing audits has to be mentioned separately in Techno-commercial proposal along with purchase details of licences and shall be cross checked with respective OEMs.
7. List of all various tools and software required for performing security testing audits has to be mentioned separately in Techno-commercial proposal along with purchase details of licences and shall be cross checked with respective OEMs.
8. Having training capabilities and conducted at least three Information Security related training assignments during the last two years.
9. Confirmation to execute the project as per the following schedule.
10. Two professionals from the project team will be allocated for on-site project implementation for a specified number of weeks.

TECHNICAL CRITERIA (QUALIFYING SCORE: 80%)

Sl No.	Particulars	Score (Total: 100%)	Remarks
1	Minimum Experience in Cyber Security and Data Protection Consultancy	5%	
2	Similar Consultancy Assignments for Telecom Operator	10%	
3	Successful Cyber Security Audit Assessments/ISO 27001 Implementations	5%	
4	Vendor Certification Requirements (ISO 9001, ISO 27001, or Equivalent)	5%	
5	Compliance to scope of work	5%	
6	Certified Auditors Requirement (CISA/CISSP/ISO 27001 Lead Auditor)	15%	
7	Tools and Software Requirement for Security Testing Audits; Licensed/Proprietary Security	15%	

	Testing & Scanning Tool Requirement.		
8	On-site professionals	20%	
9	Training Capabilities and Experience	10%	
10	Project Execution Confirmation	10%	

I / We agree to sign the Non-Disclosure Agreement, Fiduciary & Secrecy and the Do's and Don'ts in the format given in the RFP if we are assigned the job.

Signature: _____

Date: _____

(In the Capacity of:) _____

Duly authorised to sign the offer for and on behalf of the firm/Company

FINANCIAL BID

Description of Work	**Amount (Rs.)**
Auditing services regarding the assessment of cybersecurity compliance for Bhutan Telecom's Mobile Network, IT infrastructure, and Data Center services.	