TERMS OF REFERENCE for SELECTION OF CONSULTANT FOR NATIONAL CYBERSECURITY RISK ASSESSMENT (NCRA) DEPLOYMENT

Country: Bhutan

Name of Project: Accelerating Transport and Trade Connectivity in Eastern South Asia (Access) – Bhutan Project

Loan No/Credit No/ Grant No: IDA 77560 (Credit)/IDAE4310 (grant)

Assignment Title: Selection of consultancy firm for National Cybersecurity Risk Assessment (NCRA) Deployment

Activity/ Package Reference No: GovTech/CS-3/6)

1. BACKGROUND

Bhutan is accelerating its digital transformation as a critical enabler of economic diversification, private sector development, and regional integration. Guided by its 13th Five-Year Plan (2024–2029), the country is prioritizing improvements in digital connectivity to stimulate job creation, attract investment, and modernize trade systems. To support these national priorities, the World Bank partnered with the Royal Government of Bhutan (RGoB) to develop the "Accelerating Transport and Trade Connectivity in Eastern South Asia" (ACCESS) project which became effective in July 2025. As a part of the project, digital systems and infrastructure for trade will be developed to improve trade efficiency, enhance public service delivery, and stimulate economic activity while strengthening the resilience of critical systems to facilitate seamless regional trade.

Cybersecurity is a core element of ACCESS to mitigate risks from weak digital foundations by establishing a Government Security Operations Center (G-SOC), developing a Critical Information Infrastructure Protection (CIIP) plan, and implementing baseline security measures across key government systems. The rollout of the recently developed National Cybersecurity Risk Assessment (NCRA) methodology across Critical Information Infrastructure (CII) operators and other key stakeholders is also a project of importance. The NCRA methodology will provide a standardized, systematic framework for identifying, evaluating, and prioritizing cyber threats and vulnerabilities across essential national systems. This will enable operators to make informed decisions about security investments and risk mitigation, thereby significantly enhancing the overall national resilience against cyber incidents. These efforts collectively provide a comprehensive layer of protection for the new digital trade systems.

2. OBJECTIVE OF THE ASSIGNMENT

The *objective* of this assignment is to provide advisory support to the Bhutan Computer Incident Response Team (BtCIRT) for the effective rollout of the National Cybersecurity Risk Assessment (NCRA) methodology to CII operators and other key stakeholders.

Specifically, the assignment will:

- Facilitate the effective adoption of the NCRA methodology by CII operators by strengthening their capacity to conduct risk assessment through stakeholder workshops.
- Support CIIs in carrying out organizational-level risk assessments and conducting a comprehensive analysis of identified risks and threats.
- Develop and present the National Cybersecurity Risk Assessment report including the cybersecurity threat landscape with actionable recommendations.
- Equip BtCIRT to perform future NCRA rollouts by providing hands-on support, tools, and practical training throughout the implementation process.

3. SCOPE OF SERVICES

3.1. Preliminary work

Review the NCRA Methodology and NCRA Guide

As the consultancy firm supporting the implementation of Bhutan's first National Cybersecurity Risk Assessment (NCRA) in line with the country's NCRA Methodology, the firm will go through the recently developed NCRA methodology and NCRA user guide as a part of the firm's preliminary work to understand it.

The NCRA is executed through five sequential phases/steps, each comprising specific, detailed tasks:

Phase 1 - Kick-off: This step marks the initiation of the NCRA process and preparation for its implementation. It ensures that all participating institutions (CIIs) understand what is expected of them, how the process will be carried out, and the anticipated outcomes. A key focus at this stage is identifying knowledge gaps and addressing them through capacity-building workshops.

Phase 2 - Institutional Risk Assessments: This is the core step of the NCRA implementation, where CII operators conduct internal cybersecurity risk assessments, including asset identification, threat analysis, and evaluation of security controls. The level of effort required will vary depending on each CII's capacity, with tailored support provided to ensure that all CIIs are able to carry out an effective risk assessment.

Phase 3 - Submission of Risk Registers: This step constitutes the direct output of the institutional risk assessments, requiring participating institutions to consolidate their findings into standardized risk registers and submit them to the GovTech Agency.

Phase 4 - Data Analysis: This step builds on the submitted risk registers, which are aggregated and analyzed together with national threat intelligence to identify systemic risks, cross-sectoral trends, and key vulnerabilities.

Phase 5 - Dissemination of Findings: This step concludes the NCRA process by preparing and sharing the consolidated findings and recommendations. National risk assessments and threat landscape reports are produced for different audiences, ensuring that key stakeholders receive actionable insights to inform decision-making and strengthen cybersecurity resilience.

3.2. Kick-off the NCRA process

The Kick-off phase of the NCRA is key to develop and refine the scope of the first NCRA rollout in consultation with BtCIRT and other stakeholders. A detailed implementation plan that defines the assessment timeline, milestones, and deliverables will be prepared.

In order to facilitate the Kick-off phase, the firm will organize and facilitate a kick-off workshop. The workshop will introduce the NCRA process, methodology, and implications to all participating institutions. It will also help to clearly articulate the roles and responsibilities of participating institutions, sectoral regulators, and BtCIRT to ensure a shared understanding of expectations and outputs. During the workshop the firm will assess the preparedness and capacity of CIIs to carry out the organization-level risk assessment by reviewing their existing practices, technical skills, and institutional processes, and identify knowledge and capability gaps. The firm will then map overall knowledge gaps and propose or develop targeted training sessions to address them, ensuring that CII staff are adequately equipped to implement the methodology.

3.3. Institutional Risk Assessments

This is the core step of the NCRA implementation (2nd phase of the NCRA methodology), where CII operators conduct **internal cybersecurity risk assessments**, including asset identification, threat analysis, and evaluation of security controls. The level of effort required will vary depending on each CII's capacity, with tailored support provided to ensure that all CIIs are able to carry out an effective risk assessment. The consultant firm will conduct institutional risk assessments in close collaboration with CII representatives. The consultancy firm will lead the assessments while CII staff shadow the process, ensuring active participation and on-the-job learning. Groups of

institutions will be assigned a dedicated assessor(s) from the consultancy firm, responsible for guiding the institutions through all phases of the risk assessment: asset identification, threat analysis, control evaluation, and risk calculation.

The dedicated assessors will provide differentiated levels of support depending on each CII group's capacity and prior experience, as outlined in the table below.

CII Group	Existing risk assessment capacity	Type of support required	No. of dedicated assessors	Required expertise
1) Government services hosted in GovTech GDC (20 services)	No prior risk assessment experience.	Full support, step-by-step guidance; joint assessment of 20 services together (not	2	Experience in conducting cybersecurity risk assessment for a data center and its associated services.
2) Government services hosted outside GovTech GDC	No prior risk assessment experience.	Full support, step-by-step guidance.		
3) Energy Sector CIIs (9 services)	Limited capacity	Full support, step-by-step guidance.	1	Experience in conducting comprehensive cybersecurity risk assessment in the energy sector.
4) Financial Sector CIIs (17 services) **and Telecom Sector CIIs** (4 services)	Advanced capacity; already conducting risk assessments.	Although the guidance required would be on the required Risk Register format, however, an assessor will be identified to serve as the primary point of contact for addressing any clarifications or providing necessary	1	Experience in conducting cybersecurity risk assessment in telecom and banking sectors.

Please note that for the 20 critical government services hosted in GovTech's GDC, the assessment will be conducted jointly rather than as separate processes, since the systems are managed by the same technical staff.

Following the risk assessments, the participating institutions will submit **Risk Registers** as a direct output of the institutional risk assessments (phase 3 of the NCRA methodology described), requiring participating institutions to consolidate their findings into standardized risk registers and submit them to the GovTech Agency.

After the collection of the risk registers, the **data will be aggregated and analyzed** (phase 4 of the NCRA methodology described) together with relevant national and sectoral threat intelligence to enrich understanding of the external threat landscape. This data will be used to identify systemic risks, cross-sectoral trends, interdependencies, and emerging vulnerabilities that could affect multiple CIIs or critical national functions.

3.4. Preparation of reports/documents

The firm will be required to prepare reports and documents as a part of the inception, implementation and end of the project, as detailed below:

Inception Report
This report must outline its proposed approach, detailed work plan, and the methodology for supporting the NCRA rollout. The report will include a detailed implementation plan defining the assessment timeline, milestones, and deliverables.

Monthly Progress Reports
During implementation, the firm will provide monthly progress reports to BtCIRT, summarizing activities undertaken, progress against the work plan, challenges encountered, support provided to CII operators, and planned activities for the following month.

Prepare and Present National Risk Analysis Reports
At the conclusion of the NCRA process (phase 5 of the NCRA methodology described), the consultant will prepare and share the consolidated findings and recommendations. As suggested in the NCRA methodology, the NCRA process is expected to result in a **National Cybersecurity Risk Analysis report**, presented in three versions for different audiences ensuring that key stakeholders receive actionable insights to inform decision-making and strengthen cybersecurity resilience.

- ***A confidential report for senior government officials*** *to inform strategic decision-making. Contains sensitive risk data and intelligence inputs. Dissemination is restricted to authorized recipients.*
- ***An organization-focused report for those CII operators*** *identified as having significant vulnerabilities. Provides institution-specific risk assessments and tailored mitigation recommendations.*

- ***A public report*** *with only the necessary information and recommendations to raise general awareness. The report should exclude sensitive information and recommendations that could reveal existing vulnerabilities.*
- *The consultant will prepare a dedicated section under these reports on the* ***national cybersecurity threat landscape*** *providing a high-level overview of the cyber threats faced by Bhutan. This will inform policymakers, critical infrastructure operators, and the public about the most significant and evolving cyber risks of Bhutan.*

Please note that the reports may be modified and further refined during implementation.

***Dissemination of findings to the CIIs will be carried out directly by BtCIRT, with the consultancy providing technical support as needed.**

Final Report

At the conclusion of the assignment, the firm will deliver a final report to the BtCIRT team detailing the overall implementation process and documenting lessons learned from the first NCRA implementation, documenting challenges, good practices, and opportunities for improvement. It will also provide guidance and recommendations to inform and strengthen future rollout of the NCRA. The final report should also suggest updates or adjustments required for the NCRA methodology itself, to ensure its alignment with evolving cybersecurity threats and best practices.

***All outputs delivered to the client should be attached as Annexes. All the analysis, findings, and recommendations will be presented to GovTech senior management, staff, and relevant stakeholders (list of stakeholders TBD).**

3.5. Dissemination workshops/presentations

Facilitate Stakeholder Validation Workshops

The firm will organize and facilitate workshops with key stakeholders to present the consolidated findings, validate results, and gather feedback. The sessions will provide an opportunity for discussion of actionable recommendations and prioritization of next steps.

3.6. Training/knowledge transfer

Capacity Development Workshops

The consultant will deliver targeted capacity-building sessions as per the knowledge gaps identified during the kick-off phase of the NCRA methodology, using methods that allow participants to apply the learning in practice. These sessions should include

structured training and demonstrations to ensure stakeholders understand how the assessment will be implemented.

Knowledge Transfer and Mentoring to BtCIRT

The firm will be expected to provide technical assistance, capacity building, and hands-on support throughout the NCRA process, mentoring BtCIRT staff and equipping them with the tools and practical guidance needed to independently roll out the NCRA in the future. To that end, the firm will develop a short work plan that outlines a phased transfer of leadership from the consultant to BtCIRT, with clear milestones to track progress and measure success.

One dedicated team member will be assigned from the consultancy firm to lead the mentoring effort and ensure continuity.

Knowledge Transfer and Mentoring to CIIs

In addition to BtCIRT, the consultant firm will support the CIIs in supporting gap identification and mitigation planning, assisting CIIs in identifying cybersecurity gaps and vulnerabilities revealed during the risk assessments. Provide practical recommendations on potential mitigation measures, referencing international good practices where relevant, ensuring institutions understand not only their current gaps but also the options available to strengthen their resilience over time. The firm will mentor CII staff throughout the risk assessment process to ensure they understand the methodology, can apply it independently in future cycles, and internalize lessons learned.

As part of this mentoring, shadow assessors from the CIIs will document the NCRA process in detail, creating internal references and step-by-step guides to support future organizational rollouts.

3.7. Evaluation of the assignment

The consultant's performance will be primarily evaluated based on the quality of the final deliverables and their success in achieving the project's objectives. Project progress will be continuously monitored and subject to formal, scheduled assessments, including a mandatory monthly progress review or at an alternative frequency established during the inception phase.

4. DURATION OF THE ASSIGNMENT

The assignment's implementation is expected to take 40 weeks from the commencement date.

5. DATA, SERVICES AND FACILITIES TO BE PROVIDED BY THE CLIENT

The following facilities will be made available to the Consultants:

- Office facilities including meeting rooms and internet
- Transportation for visits to CII agencies related to the assignment

6. CLIENT'S INPUT AND COUNTERPART PERSONNEL

The Professional and support counterpart personnel to be assigned by the Client to the Consultant's team will be determined during the inception of the project.

7. REPORTING REQUIREMENT & TIME SCHEDULE FOR DELIVERABLES

The following table describes the deliverables and time schedule:

Sl.	Deliverables	Time Schedule
1	**Inception report** The firm will prepare an inception report, outlining its proposed approach, detailed work plan, and the methodology for supporting the NCRA rollout.	4 weeks from contract signing
2	**Kick off Workshop** The firm will launch the kick-off phase of the NCRA methodology during this workshop. The goal is to formally introduce the NCRA process, its methodology, and its implications, while simultaneously working to refine the scope of the rollout and establish the detailed	8 weeks from contract signing
3	**Capacity Development Workshops** The firm will prepare a basic risk assessment training in advance. If necessary, this training will need to be tailored to the specific needs of the participating institutions identified during the kick-off workshops.	9-12 weeks after contract signing
4	**Monthly updates** During implementation, the firm will provide monthly progress updates to BtCIRT, summarizing activities undertaken, progress against the work plan, challenges encountered, support provided to CII operators, and planned activities for the following month.	Every month after the start of implementation of the project

5	**Organizational Risk Registers** The consultancy firm will carry out the implementation of the NCRA rollout in line with the NCRA Methodology. In the process the Standardized Risk Registers will be collected for data analysis.	28 weeks from contract signing
6	**National cybersecurity risk analysis report** The firm will have 2 months to analyze the risk registers and prepare the risk analysis report. This report will be presented in three versions for different audiences. *Please note that the reports may be modified and further refined during implementation.* ● ***a confidential report for senior government officials*** *to inform strategic decision-making. Contains sensitive risk data and intelligence inputs. Dissemination is restricted to authorized recipients.* ● ***an organization-focused report for those CII operators*** *identified as having significant vulnerabilities. Provides institution-specific risk assessments and tailored mitigation recommendations.* ● ***and a public report*** *to raise general awareness.* **The consultant will prepare a section in the report on the **national cybersecurity threat landscape** providing a high-level overview of the cyber threats faced by Bhutan. This will inform policymakers, critical infrastructure*	36 weeks from contract signing
7	**Final Report (project report)** At the conclusion of the assignment, the firm will deliver **a final report** to the BtCIRT team detailing the overall implementation process, document lessons learned, and provide guidance and recommendations for future rollout of the NCRA. The final report should also suggest updates or adjustments required for the NCRA methodology itself, to ensure its alignment with evolving cybersecurity threats and best practices.	40 weeks from contract signing

*All outputs delivered to the client should be attached as Annexes.

**All the analysis, findings, and recommendations will be presented to GovTech senior management, staff, and relevant stakeholders (list of stakeholders TBD).* The date of submission of the final report to the BtCIRT is 40 weeks from contract signing.

8. PROCEDURE FOR REVIEW OF DELIVERABLES

All required deliverables must be submitted in Docs format emailed by the identified project manager for the project to the BtCIRT focal/counterpart within the stipulated deadline specified in the timeline in section 7. Any delays and its cause must be communicated much ahead of the expected deadline.

Final acceptance of deliverables will be approved through formal, documented sign-off from the Chief of the BTCIRT, Cybersecurity Division, GovTech Agency.

9. TEAM COMPOSITION & QUALIFICATION REQUIREMENTS FOR THE KEY EXPERTS WHOSE CV AND EXPERIENCE WOULD BE EVALUATED.

The table below summarizes the key experts required along with the time inputs required from the experts:

Sl. No.	Key Experts	Numbers	Time Inputs in man-months
1.	Team Leader/Project Manager	1	2
2.	Risk Analyst	1	3
3.	Risk Assessor for government CIIs	2	3
4.	Risk Assessor for energy CIIs	1	3
5.	Risk Assessor for telecom and financial CIIs	1	3
6.	Capacity Building and Knowledge Transfer Specialist	1	2

The consultant firm is expected to include the resumes of the experts who will be engaged in the consultancy work. The details of the expertise required is as follows:

1) **Team Leader/Project Manager –** Oversee the overall implementation of the NCRA roll out, and ensure timely delivery of outputs. Manage coordination with BtCIRT, and CIIs. Supervise the work of sectoral assessors and ensure methodological consistency. Lead reporting, workshops, and quality assurance of deliverables.

- Master's degree in Cybersecurity/ ICT Management/ Project Management/ Business Administration, or a related field.
- Minimum of 10 years of experience in cybersecurity and project management.
- Proven experience in managing national or sectoral cybersecurity projects.
- Demonstrated experience in conducting or rolling out cybersecurity risk assessments within organizations, and preferably in the government sector.
- Certifications such as PMP (Project Management Professional), PRINCE2, CISSP/ CISM or equivalent are preferred. Excellent verbal and written communication skills for report writing and demonstrated leadership in coordinating multi stakeholder engagements.

2) **Risk Analyst -** Lead the analytical phase of the NCRA, guide risk assessors in applying the methodology, and ensure quality and consistency of all risk registers. Responsible for aggregation and analysis of data, and preparation of the national risk analysis report.

    - A Master's or Bachelor's Degree in Computer Science/Information Technology/ Cybersecurity or equivalent.
    - Minimum of 5 years of experience in cybersecurity risk assessment and management, preferably in the government sector.
    - Experience in conducting National Cybersecurity risk assessments, compiling and synthesizing inputs from various organizations into comprehensive consolidated reports.
    - Experience preparing national or organizational risk reports.
    - Industry-recognized certifications are preferred (CISSP, CISA, CRISC, or CISM).
    - Deep understanding and experience in the implementation of risk management frameworks (ISO 27001, ISO 31000: NIST Risk Management Framework, or similar).
    - Excellent verbal and written communication skills for report writing and stakeholder presentations.

3) **Risk Assessor for government CIIs (2 experts)** - Conduct and guide institutional risk assessments across assigned government CIIs. Provide mentoring and on-the-job training to system operators and focal points. Participate in data analysis for the assessed systems.
    - A Bachelor's Degree in Computer Science/Information Technology/Cybersecurity or equivalent.
    - Industry-recognized certification is preferred (CISSP, CISA, CRISC, CISM).
    - Experience in the implementation of risk management frameworks (ISO 27001, ISO 31000: NIST Risk Management Framework, or similar).
    - Minimum 5 years of experience in cybersecurity risk assessment, preferably of data centers.

- Prior experience mentoring or training technical teams preferred.

4) **Risk Assessor for energy CIIs (1 expert) -** Conduct and guide institutional risk assessments across assigned energy sector CIIs. Provide mentoring and on-the-job training to system operators and focal points. Participate in data analysis for the assessed systems.

    - A Bachelor's Degree in Computer Science/Information Technology/Cybersecurity or equivalent
    - Industry-recognized certification is preferred (CISSP, CISA, CRISC, CISM)
    - Experience in the implementation of risk management frameworks (ISO 27001, ISO 31000: NIST Risk Management Framework, or similar)
    - Minimum 5 years of experience in organizational cybersecurity risk assessment, preferably in the energy sector.
    - Familiarity with the operational environment and key IT assets of the energy sector.
    - Prior experience mentoring or training technical teams preferred.

5) **Risk Assessor for telecom and financial CIIs (1 expert) -** Conduct and guide institutional risk assessments across assigned telecom and financial sectors CIIs. Provide mentoring and on-the-job training to system operators and focal points. Participate in data analysis for the assessed systems.

    - A Bachelor's Degree in Computer Science/Information Technology/Cybersecurity or equivalent.
    - Industry-recognized certification is preferred (CISSP, CISA, CRISC, CISM).
    - Experience in the implementation of risk management frameworks (ISO 27001, ISO 31000: Risk Management/NIST Risk Management Framework, or similar).
    - Minimum 5 years of experience in organizational cybersecurity risk assessment, preferably in the telecom and financial sector.
    - Familiarity with the operational environment and key IT assets of the telecom and financial sectors.
    - Prior experience mentoring or training technical teams preferred.

6) **Capacity Building & Knowledge Transfer Specialist (1 expert) -** Prepare and support the delivery of kick off introductory workshops. Identify knowledge gaps, design and deliver relevant training and capacity-building programs for CII representatives. Monitor and evaluate training impact.

    - A bachelor’s degree in Cybersecurity/Information Technology or equivalent, and recognized certification in education or related discipline.

- Minimum 7 years of experience in capacity development or organizational learning, preferably in ICT or cybersecurity contexts.
- Demonstrated experience designing and delivering technical training programs.
- Excellent facilitation and communication skills.

10. Selection Procedure

The Consultant will be selected following the Consultant's Qualification Selection (CQS) method as set forth in the World Bank Procurement Regulations for IPF Borrowers, September 2023.