1. **Background and Justification**

1.1 Trinidad and Tobago is one of the countries in the region most in need of technical support in facing cyber threats. The country was ranked 125 out of 182 countries on the 2020 Global Cybersecurity Index and 20th among 35 countries analysed in the Americas. At the operational level, the IDB’s 2020 Regional Cybersecurity Maturity Report found that adherence to ICT security standards had not improved from the previously assessed levels in 2016 and remained below the average threshold. These vulnerabilities have increased over time. Between March and June 2022, the country’s Cyber Security Incident Response Team (TT-CSIRT) observed a sharp increase in malicious cyber activity targeting local and regional entities. The most prominent threats, by order of impact, include ransomware; social engineering (Phishing); and malicious Insiders.

1.2 Meeting this challenge of increased target exposure and risk of cyber victimization will require interventions at the operational and policy level. TT-CSIRT led the conduct of the 2022 National Cybersecurity Risk Assessment (NCRA), which sought to assess national information infrastructure assets and resources in critical sectors and organisations that could be vulnerable to cyber security intrusion, attacks, hacking, and destabilization. The study found that 1 in 3 critical information infrastructure systems could be classified in the two highest risk categories, based on likelihood and impact. The assessment has laid the groundwork for developing Trinidad and Tobago’s first prioritised cyber risk asset register and work must now ensue on elaborating the register’s classification scheme towards ensuring the efficient allocation of cybersecurity resources, timely reporting on risk portfolios and enhanced risk management and responses for key national assets such as critical infrastructure.

1.3 Attendant with the ability enhanced risk assessment is the state’s capacity to respond effectively when a cyber incident occurs. Robust cybersecurity and cybercrime frameworks increase the likelihood of successful enforcement, investigation, and prosecution when a cyber threat is realised. However, the country’s legal frameworks regarding cybercrime and cyber security are not fully mature, due in part to public sector personnel still requiring additional training to draft, interpret and enforce cyber legislation and not being aware of how their roles impact other actors within the system. Whereas capacity building can be delivered in an institution-specific manner, good practice has established that cybersecurity legal practitioners and first responders benefit from the synergies, cross-learning and consistency in incident response models afforded by collaborative training opportunities. Building organisational knowledge and interpersonal trust in addressing

---

1 https://ttcsirt.gov.tt/threat-alert-2022/
cybersecurity and cybercrime should then redound to the benefit of key government agencies such as the Ministry of the Attorney General’s Chambers and Legal Affairs, the National Information and Communication Technology Company Limited (iGovTT), the Ministry of National Security, Ministry of Digital Transformation, Office of Disaster Preparedness and Management (ODPM), Trinidad and Tobago Defence Force (TTDF), Trinidad and Tobago Police Service (TTPS), Integrated Threat Assessment Centre (ITAC) and National Fusion Centre (NFC).

1.4 Development and implementation of critical infrastructure protection plans are critical for the effective management of cybersecurity. Appropriate mechanisms for the identification assessment and mitigation of risks to critical infrastructure are required for national security resilience.

2. Objectives

2.1. The objective of this contract is to support cyber security officials within the Ministry of National Security Trinidad and Tobago to:
   2.1.1. Conduct diagnostics of the existing framework and mechanisms for assessing cyber risk to the nation’s critical infrastructure
   2.1.2. Create a technical note with a costed action plan for risk management and response enhancements.

3. Key Activities

3.1. Identification: The Consulting Firm will catalogue all digital systems that support critical infrastructure in the country by:
   3.1.1. Meeting with cybersecurity officials and other key stakeholders identified by the Client.
   3.1.2. Documenting these systems using the characteristics such as purpose, location, data classification, the current level of vulnerability and other characteristics deemed appropriate in consultation with the Client and the IDB
   3.1.3. Prepare a draft report for consideration to the Client and the IDB
   3.1.4. Present the Final report on the findings to the Client and IDB once feedback is received.

3.2. Assessment: The Consulting Firm will then assess the organization of incident response and crisis management by
   3.2.1. Determining what measures are currently in place to respond to cyber threats.
   3.2.2. Assess the adequacy of the measures that are currently being employed by
      3.2.2.1. Identifying existing gaps and weaknesses in prevention, detection, response, and recovery capacities.
   3.2.3. Develop a draft report on findings for consideration by the Client and the IDB

Likarish, D. M. (2019, June). Collaborative training and response communities-an alternative to traditional cyber defense escalation. In 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA) (pp. 1-8). IEEE.
3.2.4. Present Final Report to the Client and the IDB once feedback is received and addressed.

3.3. **Planning:** The Consulting Firm will develop a technical note with a costed plan for risk management and response enhancement:

3.3.1. Identify the key priorities that should be addressed based on the catalogue of critical infrastructure and assessment of the organization of incident response and crisis management.

3.3.2. Identify and develop appropriate interventions to reduce the vulnerability of critical infrastructure and enhance risk response mechanisms.

3.3.3. Develop a detailed costing of each intervention for the protection of critical infrastructure.

3.3.4. Prepare a draft report on the critical infrastructure action plan for consideration by the Client and the IDB

3.3.5. Present Final Report to the Client and the IDB once feedback is received and addressed.

4. **Expected Outcome and Deliverables**

4.1. Workplan indicating timeline and methodology for the completion of activities

4.2. Draft Catalogue report from activity 3.1

4.3. Final Catalogue report from activity 3.1 after activity 3.1.3

4.4. Draft Report for activity 3.2

4.5. Final Report for activity 3.2 after activity 3.2.3

4.6. Draft report on activity 3.3

4.7. Final report on activity 3.3 after activity 3.3.4

5. **Project Schedule and Milestones**

5.1. The work shall be carried out in the span of six (6) months from the time of contract signature. The selected firm must present a proposed timeline for completion of the activities within one month of contract signature.

6. **Acceptance Criteria**

6.1. The Consulting Firm shall maintain regular communication with the point of contact at the IDB and each Client, in carrying out the activities and developing all deliverables described in this contract. The Consulting Firm shall obtain the IDB’s approval of the completion of each phase before associated payments will be processed.

6.2. A Bank representative will be copied in all communications between the Consulting Firm and the Client.

6.3. All project deliverables will be presented in professional-level English. Deliverables will be edited by native-level English speakers in order to ensure the appropriate language level.

6.4. Deliverables will be provided in editable formats (i.e., Microsoft Word, etc.), as well as any finalized formats.

6.5. **CONFIDENTIALITY**

6.5.1. The Consulting Firm and its employees or agents are aware that in discharging
their obligations pursuant to this Agreement, they may have access to privileged, confidential and/or proprietary information of the Bank or of another but in possession of the Bank including without limitation the Bank’s financial, statistical, marketing, business and personnel information, projections, plans, forecasts, reports, service capabilities or any other data or information collected and gathered in the provision of the Work and relating to the Bank’s business and any information whether written or oral identified as confidential by the Bank, is confidential information of the Bank (“Confidential Information”). Under no circumstances, except with the Bank’s express written permission, shall the Consulting Firm and its employees or its agents copy, reproduce, sell, assign, license, market, transfer, give or otherwise disclose to any person or organization, in any manner or form, now or after the expiration of the Agreement, such Confidential Information or any part thereof.

6.5.2. Upon request by the Bank or upon completion of the Work, Consulting Firm will immediately return to the Bank at Consulting Firm’s expense all Confidential Information of the Bank or Clients and any other Bank or Client documents or data and all copies thereof.

7. Supervision and Reporting

7.1. The IDB shall supervise the execution of the activities and completion of the deliverables indicated in these terms of reference and approve all payments. The point of contact at the IDB for all matters related to this contract will be the Cybersecurity Specialists of IFD/ICS.

8. Schedule of payments

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upon contract signature and approval Deliverable 4.1</td>
<td>10%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.2</td>
<td>15%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.3</td>
<td>10%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.4</td>
<td>20%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.5</td>
<td>10%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.6</td>
<td>25%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.7</td>
<td>10%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>100%</td>
</tr>
</tbody>
</table>
Activity 2.1: Cybersecurity Policy Adviser Consultancy

Background of this search: The Government of the Republic of Trinidad and Tobago (GoRTT) has identified Digital Transformation as a major focus area of development to improve the quality of services provided to all citizens. In late 2020, the GoRTT launched an ambitious digital transformation agenda as set out in its National Information and Communication Technologies (ICT) Plan 2018 – 2022. In keeping with the National ICT Plan, the mandate of the Ministry of Public Administration was expanded and rebranded as the Ministry of Public Administration and Digital Transformation with its core mission to improve public service efficiency, responsiveness, and agility through the use of digital ICT.

Trinidad and Tobago is one of the country’s in the region most in need of technical support in facing cyber threats. The country was ranked 125 out of 182 countries on the 2020 Global Cybersecurity Index and 20th among 35 countries analysed in the Americas. At the operational level, the IDB’s 2020 Regional Cybersecurity Maturity Report found that adherence to ICT security standards had not improved from the previously assessed levels in 2016 and remained below the average threshold. These vulnerabilities have increased over time. Between March and June 2022, the country’s Cyber Security Incident Response Team (TT-CSIRT) observed a sharp increase in malicious cyber activity targeting local and regional entities. The most prominent threats, by order of impact, include ransomware; social engineering (Phishing); and malicious Insiders.

Meeting this challenge of increased target exposure and risk of cybervictimization will require interventions at the operational and policy level. TT-CSIRT led the conduct of the 2022 National Cybersecurity Risk Assessment (NCRA), which sought to assess national information infrastructure assets and resources in critical sectors and organisations that could be vulnerable to cyber security intrusion, attacks, hacking and destabilization. The study found that 1 in 3 critical information infrastructure systems could be classified in the two highest risk categories, based on likelihood and impact. The assessment has laid the groundwork for developing Trinidad and Tobago’s first prioritised cyber risk asset register and work must now ensue on elaborating the register’s classification scheme towards ensuring the efficient allocation of cybersecurity resources, timely reporting on risk portfolios and enhanced risk management and responses for key national assets such as critical infrastructure.

Attendant with the ability enhanced risk assessment is the state’s capacity to respond effectively when a cyberincident occurs. Robust cybersecurity and cybercrime frameworks increase the likelihood of successful enforcement, investigation and prosecution when a cyberthreat is realised. However, the country’s legal frameworks regarding cybercrime and cyber security are not fully mature, due in part to public sector personnel still requiring additional training to draft, interpret and enforce cyber legislation and not being aware of how their roles impact other actors within the system. Building organisational knowledge and interpersonal trust in addressing cybersecurity and cybercrime should then redound to the benefit of key government agencies such as the Ministry of the Attorney General’s Chambers and Legal Affairs, the National Information and Communication Technology Company Limited (iGovTT), the Ministry of National Security, Ministry of Digital Transformation, Office of Disaster Preparedness and Management (ODPM), Trinidad and Tobago Defence Force (TTDF), Trinidad and Tobago Police Service (TTPS), Integrated Threat Assessment Centre (ITAC) and National Fusion Centre (NFC).
The Ministry of Digital Transformation is in the process of contracting a suitable qualified and resourced service provider capable of providing cybersecurity incident response services, through incident preparedness, digital forensics, detection and response, and crisis management services. Service provision will entail three elements: (i) proactive incident response services that assist the Ministry to prepare for any cyber threat that may arise while equipping them to build resilient cyber-defenses; (ii) reactive incident response services to operate during and in the aftermath of cyberattacks; and (iii) advisory services to support coherent strategy via recommendations on legislative and policy reforms as well as operational effectiveness through the design and development of manuals, simulation exercises and action plans. The Ministry will also be building cybersecurity by design into the other major programmes, including the Interoperability Programme and the e-ID Programme as the underlying software interconnects and integrates the use of data for improved service delivery and the creation of new services.

**The team's mission:** The purpose of this consultancy is to serve as the Ministry’s focal point and external oversight of its overall cyber security response posture, including the cybersecurity incident response service provider and other integral measures. The overall goal of this consultancy is that the cybersecurity incident response capabilities delivered are integrated into a broader national strategy for cybersecurity in a seamless and sustainable manner.

**What you'll do:** The Consultant will undertake the following:

- Provide high level, technical and strategic advisory services regarding cybersecurity matters.
- Facilitate and guide the technical performance of the providers of cybersecurity services to the Ministry of Digital Transformation, including the cybersecurity incident response service provider towards ensuring alignment with the National Digital Strategy.
- Review and assess the findings and recommendations of any remedial actions taken by the cybersecurity providers who are integrated into the overall cybersecurity posture for onward consideration by the Ministry’s leadership.
- Review and devise validation processes for all knowledge products produced by the various cybersecurity providers.
- Serve as an interface between the Ministry and key government agencies regarding key policy and other directives to enable adoption.
- Advise on and contribute to the re-engineering of agencies under the remit of the Ministry, as appropriate.
- Generate a report for executing preventative maintenance and sustaining compliance with the security standards.
- Produce a final report documenting cyber-resilience of the state digital apparatus and recommend next steps for policy and operational effectiveness.

**Deliverables and payments timeline:** The Consultant will deliver the following:

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>15%</td>
<td>Workplan completion</td>
</tr>
</tbody>
</table>
Skills you’ll need:

- **Citizenship:** You are either a citizen of Trinidad and Tobago or a citizen of one of our 48 member countries with residency or legal permit to work in Trinidad and Tobago.
- **Consanguinity:** You have no family members (up to fourth degree of consanguinity and second degree of affinity, including spouse) working at the IDB Group.
- **Education:** A master's degree in computer science, Computer Engineering Information Technology, or in a related discipline; and
- **Experience:** At least 15 years of relevant experience in reviewing and/or writing cybersecurity policies and procedures for Government locally, regionally and/or internationally. The consultant will have (i) demonstrated knowledge of government services that are offered to individuals, businesses and the public sector as well as (ii) expertise in IT Project Implementation, with excellent oral and written communicational skills and effective time management working with aggressive timelines.
- **Certifications:** Appropriate certifications from accredited institutions will be an asset, for example: ISO 27001 certification, Certified Ethical Hacker; Certified Information Security Manager; CompTIA Security+; Certified Information Systems Security Professional; GIAC Security Essentials; Certified Security Analyst.
- The consultant will also have the ability to translate IT terminology into clear, articulate language that non-IT colleagues can understand.
- **Languages:** English.

**Core and Technical Competencies:** Strategic, proactive, intellectually curious, solution-oriented team player. Excellent communication and influencing skills. Large-scale business process reengineering and ICT project management within the public sector. Highly organized and able to prioritize and manage multiple and varied projects. High degree of integrity while managing highly sensitive and/or confidential information.

**Opportunity Summary:**

- **Type of contract and modality:** Products and External Services Consultant PEC Lump Sum.
- **Length of contract:** 6 months.
- **Starting Date:** June 2023.
- **Location:** Trinidad and Tobago.
- **Responsible Person:** Sector Specialist - Public Management with responsibility for the Trinidad and Tobago Country Office portfolio of the Innovation in Citizens Service Division.
- **Requirements:** You must be a citizen of one of the IDB’s 48 member countries and have no family members currently working at the IDB Group.
Our culture: Our people are committed and passionate about improving lives in Latin-America and the Caribbean, and they get to do what they love in a diverse, collaborative and stimulating work environment. We are the first Latin American and Caribbean development institution to be awarded the EDGE certification, recognizing our strong commitment to gender equality. As an employee you can be part of internal resource groups that connect our diverse community around common interests.

Because we are committed to providing equal opportunities in employment, we embrace all diversity and encourage women, LGBTQ+, persons with disabilities, afro-descendants, and indigenous people to apply.

About us: At the IDB, we’re committed to improving lives. Since 1959, we’ve been a leading source of long-term financing for economic, social, and institutional development in Latin America and the Caribbean. We do more than lending though. We partner with our 48-member countries to provide Latin America and the Caribbean with cutting-edge research about relevant development issues, policy advice to inform their decisions, and technical assistance to improve on the planning and execution of projects. For this, we need people who not only have the right skills, but also are passionate about improving lives.

Our team in Human Resources carefully reviews all applications.
Component 3: Coordination Mechanisms for Cybersecurity Knowledge Creation and Dissemination
Activity 3.3 Consultancy to deploy technological platforms for information sharing, cyber-readiness assessment, visibility and preparedness

Terms of Reference

1. **Background and Justification**

I.1 Trinidad and Tobago is one of the countries in the region most in need of technical support in facing cyber threats. The country was ranked 125 out of 182 countries on the 2020 Global Cybersecurity Index and 20th among 35 countries analysed in the Americas. At the operational level, the IDB’s 2020 Regional Cybersecurity Maturity Report found that adherence to ICT security standards had not improved from the previously assessed levels in 2016 and remained below the average threshold. These vulnerabilities have increased over time. Between March and June 2022, the country’s Cyber Security Incident Response Team (TT-CSIRT) observed a sharp increase in malicious cyber activity targeting local and regional entities. The most prominent threats, by order of impact, include ransomware; social engineering (Phishing); and malicious Insiders.

I.2 Meeting this challenge of increased target exposure and risk of cyber victimization will require interventions at the operational and policy level. TT-CSIRT led the conduct of the 2022 National Cybersecurity Risk Assessment (NCRA), which sought to assess national information infrastructure assets and resources in critical sectors and organisations that could be vulnerable to cyber security intrusion, attacks, hacking and destabilization. The study found that 1 in 3 critical information infrastructure systems could be classified in the two highest risk categories, based on likelihood and impact. The assessment has laid the groundwork for developing Trinidad and Tobago’s first prioritised cyber risk asset register and work must now ensue on elaborating the register’s classification scheme towards ensuring the efficient allocation of cybersecurity resources, timely reporting on risk portfolios and enhanced risk management and responses for key national assets such as critical infrastructure.

I.3 Attendant with the ability enhanced risk assessment is the state’s capacity to respond effectively when a cyber incident occurs. Robust cybersecurity and cybercrime frameworks increase the likelihood of successful enforcement, investigation and prosecution when a cyber threat is realised. However, the country’s legal frameworks regarding cybercrime and cyber security are not fully mature, due in part to public sector personnel still requiring additional training to draft, interpret and enforce cyber legislation and not being aware of how their roles impact other actors within the system. Whereas capacity building can be delivered in an institution-specific manner, good practice has established that cybersecurity legal practitioners and first responders benefit from the synergies, cross-learning and consistency in incident response models afforded by collaborative training.

---


opportunities. Building organisational knowledge and interpersonal trust in addressing cybersecurity and cybercrime should then redound to the benefit of key government agencies such as the Ministry of the Attorney General’s Chambers and Legal Affairs, the National Information and Communication Technology Company Limited (iGovTT), the Ministry of National Security, Ministry of Digital Transformation, Office of Disaster Preparedness and Management (ODPM), Trinidad and Tobago Defence Force (TTDF), Trinidad and Tobago Police Service (TTPS), Integrated Threat Assessment Centre (ITAC) and National Fusion Centre (NFC).

I.4 There is a critical need to establish coordinated mechanisms for information sharing on cybersecurity among private and public sector entities. Technological platforms can be used to facilitate collaboration, data collection and analysis of cyber incidents, and promote real-time awareness of cyber threats.

2. Objectives

2.1. The objective of this contract is to support Trinidad and Tobago in the development of a secure mechanism for exchanging cybersecurity information among public and private sector entities.

3. Key Activities

3.1. Planning: The Consulting Firm will assess the requirements for the key stakeholders from the public and private sectors for information sharing.

3.1.1. The Consulting Firm will identify and assess the key stakeholders, both from the private and public sectors in Trinidad and Tobago with the Client and the IDB. This would involve identifying the specific requirements of each stakeholder, as well as any potential areas of conflict.

3.1.2. The Consulting Firm will conduct a thorough needs assessment to identify the specific requirements for information sharing, cyber-readiness, visibility, and preparedness. This would involve identifying any existing gaps or weaknesses in the current systems and infrastructure of both private and public entities.

3.1.3. Present draft needs assessment to the Client and IDB for feedback

3.2. Design and Deployment: The Consulting Firm will then design and deploy the appropriate technology platform to address the identified requirements together with the Client and the IDB through:

3.2.1. Platform design: The Consulting Firm the Client, and the IDB will hold a dialogue to determine the most appropriate type of platform that will allow for collaboration and communication on cybersecurity trends, prevention strategies, incident response and investigation techniques.

---

3.2.2. **Deployment**: The Consulting Firm will then develop and customize the platform in line with the Client and IDB requirements. The platform should include but not be limited to:

3.2.2.1. Interactive tools for active collaboration among private and public sectors on cyber threats
3.2.2.2. Data gathering, analysis and sharing on cyber incidents.
3.2.2.3. Shared resources for knowledge transfer and capacity building on trends, prevention strategies

3.3. **Training and Support**: The Consulting Firm will carry out a training programme for users of the platform and provide appropriate training tools including:

3.3.1. The development of videos and infographics in the use of the platform for all user types or levels.

3.4. **Testing, Evaluation and Handover**: The Consulting Firm will test the platform to ensure that it is delivering on agreed requirements and rectify any system issues before handover.

3.4.1. This will include appropriate stress testing, debugging and Client acceptance ratings.
3.4.2. Identify and assign administrative privileges and control for the platform together with the Client for handover.
3.4.3. Present the final system to the Client and the IDB

4. **Expected Outcome and Deliverables**

4.1. Workplan indicating timeline and methodology for the completion of contract activities,
4.2. Draft report on activity 3.1
4.3. Final Report on Activity 3.1
4.4. Technological platform designed and developed for activity 3.2
4.5. Training presentations and real-time support for activity 3.3
4.6. Draft report on activity 3.4
4.7. Final report on activity 3.4 after activity 3.4.2

5. **Project Schedule and Milestones**

5.1. The work shall be carried out in the span of fifteen (15) months from the time of contract signature. The selected firm must present a proposed timeline for completion of the activities within one month of contract signature.

6. **Acceptance Criteria**

6.1. The Consulting Firm shall maintain regular communication with the point of contact at the IDB and each Client, in carrying out the activities and developing all deliverables described in this contract. The Consulting Firm shall obtain the IDB’s approval of the completion of each phase before associated payments will be processed.
6.2. A Bank representative will be copied in all communications between the Consulting Firm and the Client.
6.3. All project deliverables will be presented in professional-level English. Deliverables will be edited by native-level English speakers in order to ensure the appropriate language level.

6.4. Deliverables will be provided in editable formats (i.e. Microsoft Word, etc.), as well as any finalized formats.

6.5. CONFIDENTIALITY

6.5.1. The Supplier and its employees or agents are aware that in discharging their obligations pursuant to this Agreement, they may have access to privileged, confidential and/or proprietary information of the Bank or of another but in possession of the Bank including without limitation the Bank’s financial, statistical, marketing, business and personnel information, projections, plans, forecasts, reports, service capabilities or any other data or information collected and gathered in the provision of the Work and relating to the Bank’s business and any information whether written or oral identified as confidential by the Bank, is confidential information of the Bank (“Confidential Information”). Under no circumstances, except with the Bank’s express written permission, shall the Supplier and its employees or its agents copy, reproduce, sell, assign, license, market, transfer, give or otherwise disclose to any person or organization, in any manner or form, now or after the expiration of the Agreement, such Confidential Information or any part thereof.

6.5.2. Upon request by the Bank or upon completion of the Work, Supplier will immediately return to the Bank at Supplier’s expense all Confidential Information of the Bank or Clients and any other Bank or Client documents or data and all copies thereof.

7. Supervision and Reporting

7.1. The IDB shall supervise the execution of the activities and completion of the deliverables indicated in these terms of reference and approve all payments. The point of contact at the IDB for all matters related to this contract will be the Cybersecurity Specialists of IFD/ICS.

8. Schedule of payments

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upon contract signature and approval Deliverable 4.1</td>
<td>10%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.2</td>
<td>10%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.3</td>
<td>5%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.4</td>
<td>40%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.5</td>
<td>15%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.6</td>
<td>15%</td>
</tr>
<tr>
<td>Approval of Deliverable 4.7</td>
<td>5</td>
</tr>
<tr>
<td>TOTAL</td>
<td>100%</td>
</tr>
</tbody>
</table>