TERMS OF REFERENCE

Cybersecurity Case of Studies development (individual)

1. Context and Justification

COVID-19 has accelerated the digitization of our societies, so cybersecurity has become central to the world's concerns. Cybersecurity is one of the fundamental enablers of digital transformation. Technological advances that improve our quality of life, such as telemedicine, e-health, online education, digital government, or e-commerce, would not be possible without cybersecurity measures that bring the system to an acceptable level of risk.

According to the World Economic Forum's Global Risk Report , cybersecurity is among the five most important risks faced by companies and citizens who mention the risk of their information being stolen as one of the factors that inhibits them from mass adoption of digital technologies.

The Inter-American Development Bank (IDB) and OAS assessed the evolving capacity of their member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: “Risks, Progress and the Way Forward in Latin America and the Caribbean” showed that only 13 of the 32 of the countries in the region have a national cybersecurity strategy in place.

Furthermore, only a few countries manage the exposure of their critical infrastructure –such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors– to cyberattacks. As revealed by the 2020 Report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrying findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

2. Objective

To develop the study of cybersecurity public policy development experiences with a special focus on lessons learned

3. Activities

The main activities are:

1. Identify the experience to analyze and develop a workplan to develop the case of study
2. Implement the workplan defined in activity 1
3. Share the draft of Case of Study for comments.
4. Elaborate the final document of the Case of Study and present it.

4. Deliverables

The deliverables of this consultancy are:

a) Workplan of the consultancy at 1 month of the contract
b) Draft of the Case of the study at 3 month of deliverable a)
c) Final document at 3 month of the deliverable b)

5. Consultant Requirements

Citizenship: You are a citizen of one of our 48 member countries.

Consanguinity: You have no relatives (up to the fourth degree of consanguinity and second degree of affinity, including spouse) working in the IDB Group.

Education: Graduation in: Law, Economics, Political Science, Public Administration, Sociology, International Relations and/or Engineering. Master's degree desirable.

Experience: Minimum 5 years of experience developing projects Latin American and Caribbean level on issues related to objective of the contract. Proven experience in public policy analysis.

Languages: Fluency in Spanish and English; fluency in Portuguese desirable.

6. Payment Schedule

Payment terms will be based on project milestones or deliverables. The Bank does not expect to make advance payments under consulting contracts unless a significant amount of travel is required. The Bank desires to receive the most competitive cost proposal for the services described herein.

Payment schedule	
Deliverable	**%**
deliverable a)	20%
deliverable b)	30%
deliverable c)	50%
TOTAL	100%

TERMS OF REFERENCE

Cybersecurity Public Policy Design (individual)

1. Context and Justification

COVID-19 has accelerated the digitization of our societies, so cybersecurity has become central to the world's concerns. Cybersecurity is one of the fundamental enablers of digital transformation. Technological advances that improve our quality of life, such as telemedicine, e-health, online education, digital government, or e-commerce, would not be possible without cybersecurity measures that bring the system to an acceptable level of risk.

According to the World Economic Forum's Global Risk Report , cybersecurity is among the five most important risks faced by companies and citizens who mention the risk of their information being stolen as one of the factors that inhibits them from mass adoption of digital technologies.

The Inter-American Development Bank (IDB) and OAS assessed the evolving capacity of their member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: “Risks, Progress and the Way Forward in Latin America and the Caribbean” showed that only 13 of the 32 of the countries in the region have a national cybersecurity strategy in place.

Furthermore, only a few countries manage the exposure of their critical infrastructure –such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors– to cyberattacks. As revealed by the 2020 Report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrying findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

2. Objective

To assist the countries of the region in the design of their public cybersecurity policies. This can be done in individual meetings or workshops.

3. Activities

The main activities are:

1. Develop a work plan to assist a country of the region in the design of their public policy in cybersecurity
2. Implement the workplan defined in activity 1
3. Share the drafts of the Public Policy for comments
4. Deliver the final document of the Public Policy and present it.

1. Deliverables

The deliverables of this consultancy are:

a) Workplan of the consultancy at 1 month of the contract
b) Draft of the Public Policy at 4 month of deliverable a)
c) Final document at 4 month of the deliverable b)

d) Consultant Requirements

Citizenship: You are a citizen of one of our 48 member countries.

Consanguinity: You have no relatives (up to the fourth degree of consanguinity and second degree of affinity, including spouse) working in the IDB Group.

Education: Graduation in: Law, Economics, Political Science, Public Administration, Sociology, International Relations and/or Engineering. Master's degree desirable.

Experience: Minimum 5 years of experience developing projects Latin American and Caribbean level on issues related to objective of the contract. Proven experience in public policy analysis.

Languages: Fluency in Spanish and English; fluency in Portuguese desirable.

e) Payment Schedule

Payment terms will be based on project milestones or deliverables. The Bank does not expect to make advance payments under consulting contracts unless a significant amount of travel is required. The Bank desires to receive the most competitive cost proposal for the services described herein.

Payment schedule	
Deliverable	**%**
deliverable a)	20%
deliverable b)	30%
deliverable c)	50%
TOTAL	100%

TERMS OF REFERENCE

Cybersecurity Workshop Management (firm)

1. Context and Justification

COVID-19 has accelerated the digitization of our societies, so cybersecurity has become central to the world's concerns. Cybersecurity is one of the fundamental enablers of digital transformation. Technological advances that improve our quality of life, such as telemedicine, e-health, online education, digital government, or e-commerce, would not be possible without cybersecurity measures that bring the system to an acceptable level of risk.

According to the World Economic Forum's Global Risk Report , cybersecurity is among the five most important risks faced by companies and citizens who mention the risk of their information being stolen as one of the factors that inhibits them from mass adoption of digital technologies.

The Inter-American Development Bank (IDB) and OAS assessed the evolving capacity of their member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: “Risks, Progress and the Way Forward in Latin America and the Caribbean” showed that only 13 of the 32 of the countries in the region have a national cybersecurity strategy in place.

Furthermore, only a few countries manage the exposure of their critical infrastructure –such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors– to cyberattacks. As revealed by the 2020 Report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrying findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

2. Objective

To assist the Bank in the design, coordination and moderation of 3 workshops and 3 dialogues for the development of public policies on cybersecurity.

3. Activities

The main activities are:

1. Develop a workplan for the design, coordination and moderation of workshops and dialogues
2. Design the workshops and dialogues
3. Coordinate the organization for the activities
4. Moderate the workshops and dialogues
5. Deliver a final report with the result and lessons learned of the workshops.

6. Deliverables

The deliverables of this consultancy are:

a) Workplan of the service at 1 month of the contract
b) Workshop or dialogue final reports (6)

7. Firm Requirements

Interested consulting firms should provide information indicating that they are qualified to provide the services (brochures, description of similar work, experience under similar conditions, availability of personnel with relevant expertise, etc.). In particular they should demonstrate experience in cybersecurity consulting, experience in critical infrastructure protection and public policy. Eligible consulting firms may partner as a joint venture or in a sub-consulting arrangement to enhance their qualifications. Such a partnership or joint venture will appoint one of the firms as a representative.

8. Payment Schedule

Payment terms will be based on project milestones or deliverables. The Bank does not expect to make advance payments under consulting contracts unless a significant amount of travel is required. The Bank desires to receive the most competitive cost proposal for the services described herein.

Payment schedule	
Deliverable	**%**
deliverable a)	10%
deliverable b) (6 events)	90%
TOTAL	100%

TERMS OF REFERENCE

Cybersecurity Educational Framework development (individual)

1. Context and Justification

COVID-19 has accelerated the digitization of our societies, so cybersecurity has become central to the world's concerns. Cybersecurity is one of the fundamental enablers of digital transformation. Technological advances that improve our quality of life, such as telemedicine, e-health, online education, digital government, or e-commerce, would not be possible without cybersecurity measures that bring the system to an acceptable level of risk.

According to the World Economic Forum's Global Risk Report , cybersecurity is among the five most important risks faced by companies and citizens who mention the risk of their information being stolen as one of the factors that inhibits them from mass adoption of digital technologies.

The Inter-American Development Bank (IDB) and OAS assessed the evolving capacity of their member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: “Risks, Progress and the Way Forward in Latin America and the Caribbean” showed that only 13 of the 32 of the countries in the region have a national cybersecurity strategy in place.

Furthermore, only a few countries manage the exposure of their critical infrastructure –such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors– to cyberattacks. As revealed by the 2020 Report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrying findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

2. Objective

To assist countries in the region in the development of cybersecurity educational frameworks. Including implementation models.

3. Activities

The main activities are:

1. Develop a workplan to develop a knowledge material for the implementation of cybersecurity measures.
2. Implement the workplan defined in activity 1
3. Share the drafts of the Cybersecurity Knowledge Material for comments
4. Deliver the final document of the Cybersecurity Knowledge Material and present it.

5. Deliverables

The deliverables of this consultancy are:

a) Workplan of the consultancy at 1 month of the contract
b) Draft of the Educational Framework at 4 month of deliverable a)
c) Final document at 4 month of the deliverable b)

c) Consultant Requirements

Citizenship: You are a citizen of one of our 48 member countries.

Consanguinity: You have no relatives (up to the fourth degree of consanguinity and second degree of affinity, including spouse) working in the IDB Group.

Education: Graduation in: Law, Economics, Political Science, Public Administration, Sociology, International Relations and/or Engineering. Master's degree desirable.

Experience: Minimum 5 years of experience in cybersecurity projects Latin American and Caribbean. Proven experience in knowledge material development.

Languages: Fluency in Spanish and English; fluency in Portuguese desirable.

d) Payment Schedule

Payment terms will be based on project milestones or deliverables. The Bank does not expect to make advance payments under consulting contracts unless a significant amount of travel is required. The Bank desires to receive the most competitive cost proposal for the services described herein.

Payment schedule	
Deliverable	**%**
deliverable a)	20%
deliverable b)	30%
deliverable c)	50%
TOTAL	100%

TERMS OF REFERENCE

Cybersecurity Knowledge material development (individual)

1. Context and Justification

COVID-19 has accelerated the digitization of our societies, so cybersecurity has become central to the world's concerns. Cybersecurity is one of the fundamental enablers of digital transformation. Technological advances that improve our quality of life, such as telemedicine, e-health, online education, digital government, or e-commerce, would not be possible without cybersecurity measures that bring the system to an acceptable level of risk.

According to the World Economic Forum's Global Risk Report , cybersecurity is among the five most important risks faced by companies and citizens who mention the risk of their information being stolen as one of the factors that inhibits them from mass adoption of digital technologies.

The Inter-American Development Bank (IDB) and OAS assessed the evolving capacity of their member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: “Risks, Progress and the Way Forward in Latin America and the Caribbean” showed that only 13 of the 32 of the countries in the region have a national cybersecurity strategy in place.

Furthermore, only a few countries manage the exposure of their critical infrastructure –such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors– to cyberattacks. As revealed by the 2020 Report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrying findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

2. Objective

Develop knowledge material for the implementation of cybersecurity measures.**Activities**

The main activities are:

1 Develop a work plan to assist a country of the region in the design of their educational in cybersecurity
2 Implement the workplan defined in activity 1
3 Share the drafts of the Educational Cybersecurity Framework for comments
4 Deliver the final document of the Educational Cybersecurity Framework and present it.

3. Deliverables

The deliverables of this consultancy are:

a) Workplan of the consultancy at 1 month of the contract
b) Draft of the Educational Framework at 4 month of deliverable a)
c) Final document at 4 month of the deliverable b)

4. Consultant Requirements

Citizenship: You are a citizen of one of our 48 member countries.

Consanguinity: You have no relatives (up to the fourth degree of consanguinity and second degree of affinity, including spouse) working in the IDB Group.

Education: Graduation in: Law, Economics, Political Science, Public Administration, Sociology, International Relations and/or Engineering. Master's degree desirable.

Experience: Minimum 5 years of experience developing cybersecurity or educational projects Latin American and Caribbean. Proven experience in educational framework analysis.

Languages: Fluency in Spanish and English; fluency in Portuguese desirable.

5. Payment Schedule

Payment terms will be based on project milestones or deliverables. The Bank does not expect to make advance payments under consulting contracts unless a significant amount of travel is required. The Bank desires to receive the most competitive cost proposal for the services described herein.

Payment schedule	
Deliverable	**%**
deliverable a)	20%
deliverable b)	30%
deliverable c)	50%
TOTAL	100%

TERMS OF REFERENCE

Cybersecurity training development and delivery (firm)

1. Context and Justification

COVID-19 has accelerated the digitization of our societies, so cybersecurity has become central to the world's concerns. Cybersecurity is one of the fundamental enablers of digital transformation. Technological advances that improve our quality of life, such as telemedicine, e-health, online education, digital government, or e-commerce, would not be possible without cybersecurity measures that bring the system to an acceptable level of risk.

According to the World Economic Forum's Global Risk Report, cybersecurity is among the five most important risks faced by companies and citizens who mention the risk of their information being stolen as one of the factors that inhibits them from mass adoption of digital technologies.

The Inter-American Development Bank (IDB) and OAS assessed the evolving capacity of their member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: “Risks, Progress and the Way Forward in Latin America and the Caribbean” showed that only 13 of the 32 of the countries in the region have a national cybersecurity strategy in place.

Furthermore, only a few countries manage the exposure of their critical infrastructure –such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors– to cyberattacks. As revealed by the 2020 Report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrying findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

2. Objective

To develop and deliver advanced cybersecurity training courses. Practical courses should be carried out using CyberRange platforms.

3. Activities

The main activities are:

1. Develop a workplan for the design and the delivery of the training
2. Elaboration of detailed cybersecurity training programs, the content, class-by-class topics, the necessary prior knowledge requirements and recommended bibliography should be made explicit.
3. Deliver the training

4. Deliverables

The deliverables of this consultancy are:

a) Workplan of the service at 1 month of the contract
b) Training programs at 3 month of the activity a)
c) Training delivery at 12 month of the activity b)

5. Firm Requirements

Interested consulting firms should provide information indicating that they are qualified to provide the services (brochures, description of similar work, experience under similar conditions, availability of personnel with relevant expertise, etc.). In particular they should demonstrate experience in cybersecurity consulting, experience in critical infrastructure protection and public policy. Eligible consulting firms may partner as a joint venture or in a sub-consulting arrangement to enhance their qualifications. Such a partnership or joint venture will appoint one of the firms as a representative.

6. Payment Schedule

Payment terms will be based on project milestones or deliverables. The Bank does not expect to make advance payments under consulting contracts unless a significant amount of travel is required. The Bank desires to receive the most competitive cost proposal for the services described herein.

Payment schedule	
Deliverable	**%**
deliverable a)	10%
deliverable b)	30%
Deliverable c)	60%
TOTAL	100%

TERMS OF REFERENCE

Pilot Project Implementation (firm)

1. Context and Justification

COVID-19 has accelerated the digitization of our societies, so cybersecurity has become central to the world's concerns. Cybersecurity is one of the fundamental enablers of digital transformation. Technological advances that improve our quality of life, such as telemedicine, e-health, online education, digital government, or e-commerce, would not be possible without cybersecurity measures that bring the system to an acceptable level of risk.

According to the World Economic Forum's Global Risk Report, cybersecurity is among the five most important risks faced by companies and citizens who mention the risk of their information being stolen as one of the factors that inhibits them from mass adoption of digital technologies.

The Inter-American Development Bank (IDB) and OAS assessed the evolving capacity of their member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: “Risks, Progress and the Way Forward in Latin America and the Caribbean” showed that only 13 of the 32 of the countries in the region have a national cybersecurity strategy in place.

Furthermore, only a few countries manage the exposure of their critical infrastructure –such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors– to cyberattacks. As revealed by the 2020 Report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrying findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

2. Objective

To implement Pilot Project for the beneficiaries countries of advanced cybersecurity techniques and technologies.

3. Activities

The main activities are:

1. Develop a workplan for the design and implementation of the pilot project.
2. Execute de workplan for the activity 1)
3. Elaborate a final report of the pilot project including lesson learned.

4. Deliverables

The deliverables of this consultancy are:

a) Workplan of the service, at 1 month of the contract
b) Final execution pilot project report at 10 months of the deliverable a)

1. Firm Requirements

Interested consulting firms should provide information indicating that they are qualified to provide the services (brochures, description of similar work, experience under similar conditions, availability of personnel with relevant expertise, etc.). In particular they should demonstrate experience in cybersecurity consulting, experience in critical infrastructure protection and public policy. Eligible consulting firms may partner as a joint venture or in a sub-consulting arrangement to enhance their qualifications. Such a partnership or joint venture will appoint one of the firms as a representative.

2. Payment Schedule

Payment terms will be based on project milestones or deliverables. The Bank does not expect to make advance payments under consulting contracts unless a significant amount of travel is required. The Bank desires to receive the most competitive cost proposal for the services described herein.

Payment schedule	
Deliverable	**%**
deliverable a)	30%
deliverable b)	70%
TOTAL	100%