ASEAN AUSTRALIA SMART CITIES TRUST FUND
Asian Development Bank

Australian Government
Department of Foreign Affairs and Trade

ADB

SMART CITIES Guided Learning Programme

Home Exercise 2

ASEAN Australia Smart Cities Trust Fund (AASCTF)

October 2022

Begin Home Exercise

Guided Learning Programme

ASEAN
AUSTRALIA
SMART CITIES
TRUST FUND
Asian Development Bank

BEFORE YOU CONTINUE...

Please download this file onto your computer or mobile device before working on this exercise to avoid overwriting the original file.

Instructions on how to submit your finished work will be provided at the end of this document.

If you encounter any issues with this exercise, please contact Kristine Lucero at kjl@ramboll.com or via WhatsApp/Telegram at +639171702953.

Next

Guided Learning Programme

Welcome

Guided Learning Programme

The key to unlocking a smart, livable city is data management.

Most cities today generate ample amounts of data from services and operations that power the function of a city; however, this data is not maximized enough to inform urban planning and decision-making.

The growing concern about data privacy and security also hampers the use of digital systems and data collection.

What can cities do to ensure these vital information are not wasted? How can data governance be improved, and how can it lead to more livable cities?

These are some of the questions that will be addressed in the Guided Learning Programme (GLP) of the ASEAN Australia Smart Cities Trust Fund (AASCTF)

Next

Guided Learning Programme

The programme structure

This programme is aimed at professionals who are starting their journey working with **urban data** and will be responsible for planning data projects in their city.

The programme consists of three webinars with supplementary coursework to be completed by the specific deadline. You are now to begin the second home exercise.

Home Exercise 1

Data Collection and Storage

Home Exercise 2

Data Governance and Security

Home Exercise 3

Data Analysis and Decision Making

< Back Next >

Home Exercise 2

Home Exercise 2 – Data Governance and Security

The second home exercise in the series is called ‘Data Governance and Security’. In this exercise, we will address the key considerations on data governance and data security when preparing an initial proposal.

We kindly ask you to reflect on the questions being asked in the home exercise. Note that the output of the course will be for you to have developed a basic urban data project proposal.

Home Exercise 1

Data Collection and Storage

Home Exercise 2

Data Governance and Security

Home Exercise 3

Data Analysis and Decision Making

< Back   Next >

Home Exercise 2

Types of slides

This home exercise is composed of three types of content: Warm-ups, activities, and reflections.

They are labelled as such on the left sidebar of each slide.

EXAMPLE
WARMUP

Slides featuring this panel contains a warm-up activity to help you draw connections between the big ideas of each lesson and your own life

EXAMPLE
ACTIVITY

Slides featuring this panel contain the main activity of each lesson in which you will apply the tools and strategies from the course to real-life experiences

EXAMPLE
REFLECT & SUBMIT

REQUIRED SUBMISSION

Slides featuring this panel contain the final reflection activity of each lesson. You will submit your answers from any slides tagged with the red submission button.

< Back
Next >

Guided Learning Programme

ASEAN
AUSTRALIA
SMART CITIES
TRUST FUND
Asian Development Bank

Welcome

Home Exercise 2

In this home exercise, you will be introduced to how data governance works in a city context and how to apply it in your organisation, as well as the challenges that cities face in making accurate data available and maintaining it in a secure environment.

- Get a general understanding of the significance of data governance and security in smart cities

- Understand the concepts and principles of data protection and security and why it is important to build and maintain strong data organisations

- Be introduced to actual methods for data protection and security requirements.

Type: Training
Module length: 60 min

Start Home Exercise

Data Governance in cities
Introduction

ASEAN AUSTRALIA SMART CITIES TRUST FUND
Asian Development Bank

Urban Data in Smart Livable Cities

Realising the full potential of smart cities is done through the enablement of data sharing. This is in terms of municipalities sharing data with citizens and companies as well as vice versa. The sharing of data between different stakeholders and data generated from information and communication technologies such as IoT sensors in the urban environment increase the volume, variety and velocity of urban data. This creates new possibilities and opportunities for new business cases and for improving cities. However, it also creates new socio-technical challenges and risks that, if not managed appropriately, can compromise the rights, privacy and security of citizens.

At its core of data governance is how a city's performance and quality of life can benefit from data-enabled technologies without compromising privacy. Cities are built and operated on data, much of it personal in nature. Consider the information that cities may store about you: your address, birthdate, medical history, income, criminal background, voter registration, permit requests, driving record, fines, education, and more.

< Back

Next >

Data Governance in cities
Introduction

The prevalent challenges related to smart city data management are: (continued on next page)

Data privacy

Urban data associated to individuals, such as information about citizens collected through tracking of cellular/WiFi activities of their phones, can compromise the rights and privacy of individuals, especially if this data is collected, managed and used inappropriately according to privacy laws and without citizens' consent.

Cyber-security

The increased use of Information Communication Technologies such as IoT sensors also creates new threats for cyber-security attacks. This can present itself as, e.g., attempts to get access to valuable information on the city and its citizens or as attacks to crucial infrastructure such as a city's energy grid

< Back
Next >

Data Governance in cities
Introduction

The prevalent challenges related to smart city data management are:

Data quality

→ Missing, erroneous, inconsistent or inaccurate data can compromise the validity, reliability and trustworthiness of the data as a resource for decision-making, actions and automatization

Data interoperability

← Urban data can come from a variety of sources, from social media to Internet-of-Things (IoT) devices, which can present data in variety of formats. This can be due to the nature of the data (e.g., structured or unstructured data), the selected communication infrastructure between device and data storage (e.g., LoraWan, SigFox, NB-IoT) and the ontology used in describing how data is stored and structured in data storage platforms. Thus, these varieties can greatly challenge data exchange between different data storage platforms or the linking of data across different sources in a common data environment.

Data Governance in cities
Introduction

Appropriately managing these challenges and threats requires an effective data governance framework or program. This is whether the program is implemented at a city-scale level or on a specific smart city project. Data governance is considered the core of data management. It binds the other data management areas, such as data analytics, data architecture, data interoperability.

Data governance can be described as

> “The discipline of exercising authority and control (planning, monitoring and enforcement) over the management of data assets through formal oversights of people, process and technologies.”

Consequently, data governance focuses on the rules, processes and resources for the execution of data management. This means that data governance defines the organisation for data management and specifies which principles, standards and policies the organisation has to follow for it to succeed with the vision and goals set for the data management and eventually drive the vision set for the smart city.

< Back Next >

Data Governance in cities
Introduction

Data governance aims to support the various members in the smart city ecosystem to collaborate effectively, e.g., through transparent data sharing; to clarify the roles and responsibilities of these members for managing data assets; and to help them “do their jobs” by providing them resources about data assets and a way to escalate arisen data issues.

In other words, data governance needs to clarify the WHO and HOW of all data management related aspects such as maintenance and support of data storage, consent to use data, data anonymization, data access, data sharing and data encryption. Implementing and managing data governance for smart city, requires a well-defined data governance program.

< Back Next >

INTRODUCTION

WARMUP

TIME: 5 minutes

REQUIRED MATERIALS: None

A Smart Livable City is a Cybersecure City

Overview

How would you define the level of cyber security in your city?

Type your answer here…

- **Initial** – the starting point for a City to begin to agree and scope a capability
- **Under Development** – the capability is agreed by all parties involved, goals, objectives, requirements and planning implemented
- **Defined** – the capability is defined and implemented by all parties
- **Capable** – the capability is quantitatively managed in accordance with agreed-upon metrics.
- **Efficient** – capability management includes optimisation and continuous improvement.

< Back **Next >**

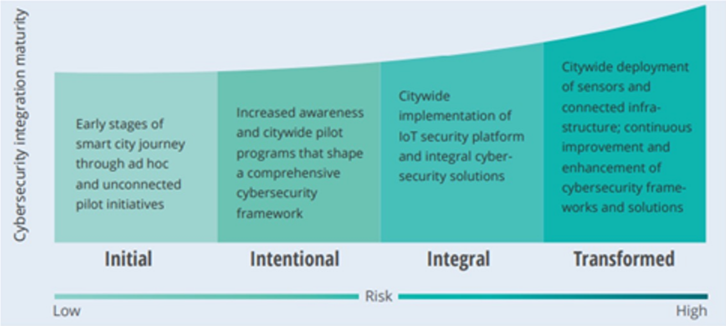
Data Governance Principles

Smart city scope and data governance principles

There are several approaches and frameworks to define and manage a data governance program for a smart city. But, overall, they share similar components described in this module.

The level of formality and the decision to define a comprehensive data governance program depend on how experienced and mature the city and its organisation is related to data and ICT management. It is recommended to start at a small scale and evolve the data governance program over time. Consequently, it becomes important to establish the current scope of the data governance program as to appropriately set the direction towards realizing the defined smart city vision. The scope can be:

- Implementing a data governance program for local smart city projects before scaling it to a city-wide program.
- Implementing a data governance program for shared data, or specifically privacy- or security-sensitive urban data.



Initial: Early stages of smart city journey through ad hoc and unconnected pilot initiatives

Intentional: Increased awareness and citywide pilot programs that shape a comprehensive cybersecurity framework

Integral: Citywide implementation of IoT security platform and integral cyber-security solutions

Transformed: Citywide deployment of sensors and connected infra-structure; continuous improvement and enhancement of cybersecurity frame-works and solutions

https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Report_making_smart_cities_cyber_secure.pdf

< Back
Next >

Data Governance Principles

When the scope is specified, the next step is to formulate data governance principles for the specified scope. Data governance principles are intended to align or affect the behaviours of members in the smart city organisation towards realizing the defined smart city vision. Consequently, defining these principles should be done by involving the relevant stakeholders and by keeping the defined smart city vision in mind.

The activity of jointly defining the principles can especially be helpful to clarify disagreements as well as reaching agreement about data governance concepts. Specifically, the latter will be important in order to have success later when agreeing on specific policies. The following provides some suggestions for governance principles for smart cities based, i.a., on Johnson et al. (2022, J. L. & Mob. 1):

- Balancing government involvement and privatization
- Considering smart city project aims in connection to surveillance concerns and citizens' privacy
- Achieve public trust through transparency and accountability
- Promote data sharing and collaboration
- Securing vulnerable ICT infrastructure against unintentional or deliberate misuse of urban data.

< Back Next >

Data Governance Organisation and Authority

Organisation and Authority

An important component of a data governance program is to identify stakeholders and establish the organisation that are benefitting, contributing and accountable for management of urban data assets. The organisation should include stakeholders from the four stakeholder-groups:

Civic Authorities

Academia & Research Institutes

Private Businesses & Industry

Citizens

Before establishing the data governance organisation, it is important to determine the balance between private and public sector involvement in managing smart city projects. On the one end of the spectrum, the local government is responsible for managing all ICT infrastructure with little or no involvement of private stakeholders. On the other end of the spectrum, the local government promotes private businesses to implement new technologies part of smart cities, and limits public involvement and rejects regulations that can hinder private businesses to provide benefits to the local community. Deciding which level is right depends on the maturity level of the local government to manage data governance and ICT technologies in the city; the desired level of control and authority of the urban data; local laws and regulations; political programs; the opinion of citizens and local community; etc.

< Back   Next >

Data Governance
Guidelines, standards and policies

Guidelines, standards and policies

Defining the data governance principles is the first step towards actionable and formalised data governance. As mentioned earlier, it is important to decide on the level of formality for the data governance based on the maturity and experience level of the city to manage data and ICT. There are some data management areas that are regulated by national or local laws or policies such as data privacy (e.g., GDPR). These needs to be included in the data governance program for a smart city project regardless of the formality level as to ensure the project is compliant with local laws and policies. However, there are other areas not covered by public laws or policies that need to be defined by the smart city project organisation. This can include the ethical use of data, standards for data quality assurance, security risk assessment of ICT projects, standards for using meta data for shared urban data, etc.

Consequently, one can start of by defining guidelines for these areas before formalizing them into policies and mandatory standards. It is important to include relevant ICT, data and subject matter experts as well as industry partners when deciding on guidelines, policies or standards for smart city projects.

The part of this home exercise provides an overall description of defining guidelines, standards and policies for data privacy and security.

If a city-wide data governance program is implemented, then it is important to decide a procedure on how guidelines, policies and standards need to be assured and enforced across smart city projects. Again, the extent of this procedure depends on the decided formality level. A less informal procedure would be that internal project members ensure smart city projects are compliant with data governance guidelines. A more formal approach is to have a smart city committee assessing whether a smart city project complies with policies.

< Back Next >

EXAMPLE

ACTIVITY

TIME: 10 minutes

REQUIRED MATERIALS: None

What Makes Your City Cybersecure?

Activity

Reflect on which initiatives that your city has implemented to make your city cybersecure?

Here are some examples:

- *Ad hoc and unconnected pilot initiatives with little to no cybersecurity framework applied*
- *Citywide pilot programs that shape a comprehensive cybersecurity framework with a cyber security strategy*
- *Citywide implementation of IoT security platform and integral cybersecurity solutions*
- *Citywide deployment of sensors and connected infrastructure with continuous improvement and enhancement of cyber security frameworks and solutions*

My city has done following to make the city cybersecure:

Type your answer here…

< Back Next >

Importance of cybersecurity and data privacy

The increasing implementation and use of ICT and urban data in decision-making in different sectors such as buildings, energy, finance and health care creates new opportunities to improve the quality and life of citizens and businesses. However, the prevalence and increased reliance of technologies and data also introduce new risks and threats to the safety, security and privacy of individuals. Cybersecurity and privacy is a particularly dynamic domain in data management. Ill-intentional people are constantly trying to find new ways to exploit vulnerabilities in software and hardware security to obtain access and control of sensitive information about cities, businesses and citizens.

The lack of focus and priority on cybersecurity and privacy in city operation can have dire consequences on financial costs, organizational credibility, operation of critical city infrastructure (e.g., energy, transportation and health care) and the lives of individuals. Consequently, incorporating cybersecurity and data privacy in the smart city strategy and data governance program is crucial for creating safe and secure smart livable cities.

Many efforts are taken place by governmental and research institutes to define industry standards, regulations and laws to address cybersecurity and privacy issues and concerns. For example, the National Institute of Standards and Technology (NIST) provides guidance and frameworks on cybersecurity for U.S. federal agencies, which is also being deployed by private organisations. Another example is the European Union's General Data Protection Regulation (GDPR), which is a law that’s being enforced across member nations to protect the personal data of EU citizens.

NIST
Communications Technology Laboratory / Smart Connected Systems Division

General Data Protection Regulation

< Back Next >

Data Privacy & Security Principles

Principles of data privacy

Data privacy and security should be considered jointly as they support one another. Data privacy is considered as the practice of individual control over personal information. The notion of privacy is debated by philosophers, lawyers, sociologists, etc., thus the term per se has no consensus definition. Nevertheless, legislative acts or laws such as the EU's GDPR or the U.S Department of Homeland Security's Fair Information Practice Principles (FIPPs) defines data privacy principles that constitutes data privacy. Some of these are mentioned below:

- Transparency and fairness - Data processing of personal information must be lawful, fair and transparent to the individual.
- Individual participation - Individuals are in involved in the process of using their personal identifiable information (PII). This means, among others, seeking individual consent and providing individuals appropriate access to and control of their own data.
- Purpose limitation & data minimization – Only collecting, processing, storing and using PII that is directly relevant and necessary to accomplish the specified purposes.
- Integrity and confidentiality – Ensuring the security, reliability and confidentiality of PII so as it is accurate, relevant, timely and complete.
- Accountability – Ultimately the person responsible for data management in an organization is responsible for compliance with data privacy principles (for example, organisations based in EU need to comply with GDPR). This means they need to incorporate procedures for auditing, define standards and guidelines and provide training to all members of the organisation who use PII.

PII is personal data that can be used to identify a person either alone or in combination with other information that directly or indirectly is linked to a specific person.

< Back Next >

Data Security
Organisation and authority

Organisation and authority

Drawing upon the overall structure for a data governance program, introduced in the previous chapter, cybersecurity and data privacy is implemented by establishing an organisation responsible for defining, planning and overseeing cybersecurity and data privacy of smart city projects. Different standards, frameworks and approaches exist defined by governmental and/or national research institutes. It is therefore important that you base the cybersecurity and privacy frameworks for your smart city project on these existing frameworks. The following should be considered as recommendations and examples of cybersecurity and data privacy programs.

It is recommended to define cybersecurity and privacy principles, guidelines and eventually policies for use across smart city projects. Following the organisational hierarchy of a data governance program, a similar structure can be defined for the organisation responsible for planning, implementing and overseeing cybersecurity and privacy. This entails hiring a Chief Information Security Officer (CISO) that has the authority to make city-wide decisions related to cybersecurity and privacy. The CISO will be responsible for creating a cybersecurity strategy for the city as well as developing and operationalising processes, policies, controls, etc. related to privacy and security across smart city projects. The CISO can be further supported by a management and/or operation team responsible for the implementation of security and privacy policies and processes within specific “departments” or “units” in the city (e.g., smart transportation, smart energy, smart healthcare, etc.) and for specific technologies and information systems (e.g., infrastructure technology for datahubs for shared urban data, laptops, phones), respectively. At project level, a security and privacy expert should be involved to plan, implement and oversee privacy and security aspects of the specific smart city project.

< Back Next >

Cyber Trust Mark

The Cyber Trust mark is a cybersecurity certification for organisations with more extensive digitalised business operations. It is targeted at larger or more digitalised organisations as these organisations are likely to have higher risk levels which require them to invest in expertise and resources to manage and protect their IT infrastructure and systems. The Cyber Trust mark adopts a risk-based approach to guide organisations to understand their risk profiles and identify relevant cybersecurity preparedness areas required to mitigate these risks.

The Cyber Trust mark serves as a mark of distinction for organisations to prove that they have put in place good cybersecurity practices and measures that are commensurate with their cybersecurity risk profile.

Why should city organisations use this?

- Signifies a mark of distinction to recognise organisations as trusted partners with robust cybersecurity
- Provides a pathway to international cybersecurity standards (e.g. ISO/IEC 27001)
- Provides a guided approach for your organisation to assess cybersecurity risks and preparedness
- Takes on a risk-based approach to meet your organisation's needs without over-investing

https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-certification-for-organisations/cyber-trust-mark

Cyber Trust mark

About Cybersecurity Certification Scheme | Cyber Essentials | Cyber Trust

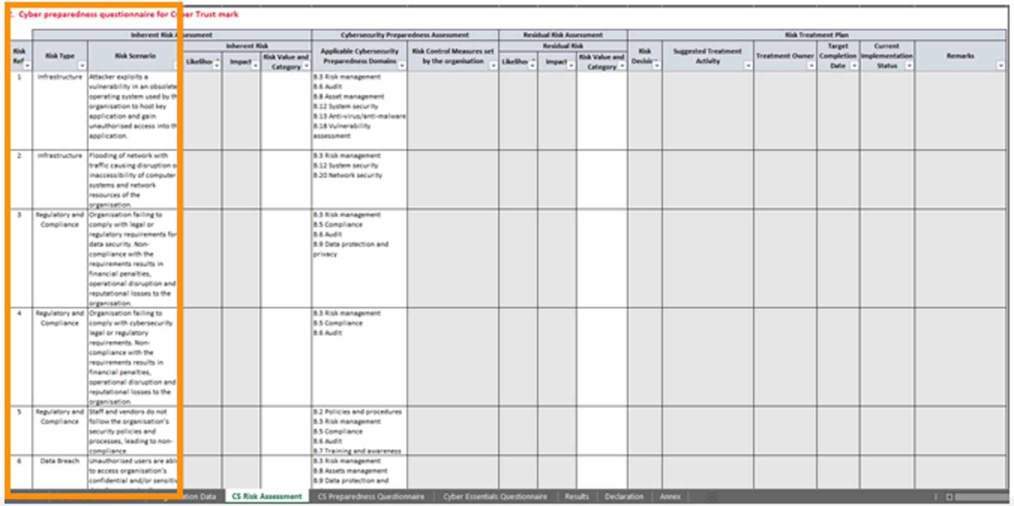
< Back
Next >

Data Security
Cybersecurity Risk Assessment

Cyber Trust Mark

The Cyber Trust Mark comes with a recommended risk assessment template "CS Risk Assessment" in the Self-Assessment Excel Template. This will be used for the home exercise. The risk self-assessment consists of:

1) 25 key cyber risks to assess
2) 6 types of cyber risks {Data Breach, Human Factor, Infrastructure, Physical Security, Regulatory and Compliance, Supply Chain}



Cyber preparedness questionnaire for Cyber Trust mark

	Inherent Risk Assessment					Cybersecurity Preparedness Assessment		Residual Risk Assessment			Risk Treatment Plan					
			Inherent Risk					Residual Risk								
Risk Ref	Risk Type	Risk Scenario	Likeliho	Impact	Risk Value and Category	Applicable Cybersecurity Preparedness Domains	Risk Control Measures set by the organisation	Likeliho	Impact	Risk Value and Category	Risk Decisi	Suggested Treatment Activity	Treatment Owner	Target Completion Date	Current Implementation Status	Remarks
1	Infrastructure	Attacker exploits a vulnerability in an obsolete operating system used by th organisation to host key application and gain unauthorised access into th application.				B.3 Risk management B.6 Audit B.8 Asset management B.12 System security B.13 Anti-virus/anti-malware B.18 Vulnerability assessment										
2	Infrastructure	Flooding of network with traffic causing disruption o inaccessibility of computer systems and network resources of the organisation.				B.3 Risk management B.12 System security B.20 Network security										
3	Regulatory and Compliance	Organisation failing to comply with legal or regulatory requirements for data security. Non-compliance with the requirements results in financial penalties, operational disruption and reputational losses to the organisation.				B.3 Risk management B.5 Compliance B.6 Audit B.9 Data protection and privacy										
4	Regulatory and Compliance	Organisation failing to comply with cybersecurity legal or regulatory requirements. Non-compliance with the requirements results in financial penalties, operational disruption and reputational losses to the organisation.				B.3 Risk management B.5 Compliance B.6 Audit										
5	Regulatory and Compliance	Staff and vendors do not follow the organisation's security policies and processes, leading to non-compliance.				B.2 Policies and procedures B.3 Risk management B.5 Compliance B.6 Audit B.7 Training and awareness										
6	Data Breach	Unauthorised users are abl to access organisation's confidential and/or sensitiv				B.3 Risk management B.8 Assets management B.9 Data protection and										

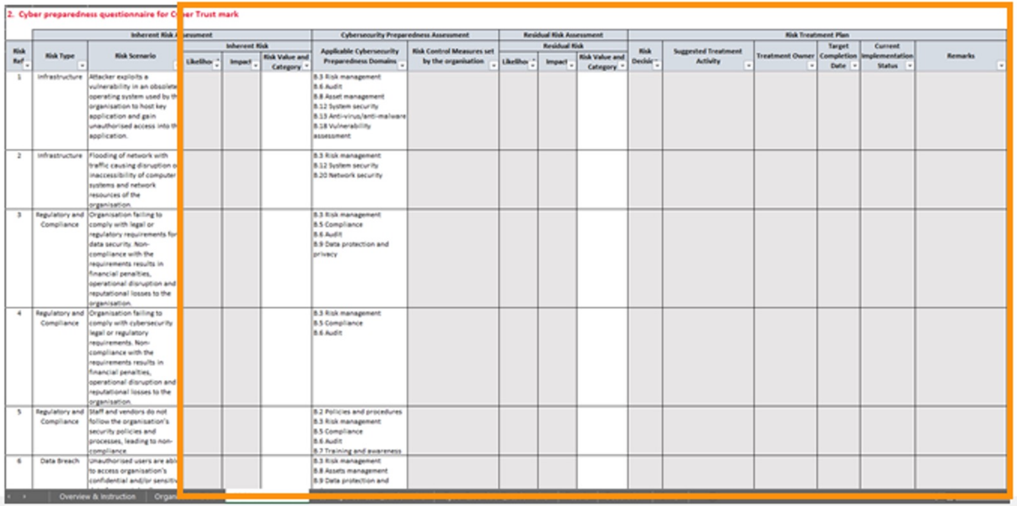
< Back   Next >

Data Security
Cybersecurity Risk Assessment

ASEAN AUSTRALIA SMART CITIES TRUST FUND
Asian Development Bank

Cyber Trust Mark

3) An overview of inherent risks and residual risks after identifying risk control measures across 22 domains
4) Risk treatment plan so that projects can plan, budget and implement additional controls to lower the risks



2. Cyber preparedness questionnaire for Cyber Trust mark

	Inherent Risk Assessment					Cybersecurity Preparedness Assessment		Residual Risk Assessment			Risk Treatment Plan					
Risk Ref	Risk Type	Risk Scenario	Inherent Risk			Applicable Cybersecurity Preparedness Domains	Risk Control Measures set by the organisation	Residual Risk			Risk Decisio	Suggested Treatment Activity	Treatment Owner	Target Completion Date	Current Implementation Status	Remarks
			Likeliho	Impact	Risk Value and Category			Likeliho	Impact	Risk Value and Category						
1	Infrastructure	Attacker exploits a vulnerability in an obsolete operating system used by th organisation to host key application and gain unauthorised access into th application.				B.3 Risk management B.6 Audit B.8 Asset management B.12 System security B.13 Anti-virus/anti-malware B.18 Vulnerability assessment										
2	Infrastructure	Flooding of network with traffic causing disruption o inaccessibility of computer systems and network resources of the organisation.				B.3 Risk management B.12 System security B.20 Network security										
3	Regulatory and Compliance	Organisation failing to comply with legal or regulatory requirements for data security. Non-compliance with the requirements results in financial penalties, operational disruption and reputational losses to the organisation.				B.3 Risk management B.5 Compliance B.6 Audit B.9 Data protection and privacy										
4	Regulatory and Compliance	Organisation failing to comply with cybersecurity legal or regulatory requirements. Non-compliance with the requirements results in financial penalties, operational disruption and reputational losses to the organisation.				B.3 Risk management B.5 Compliance B.6 Audit										
5	Regulatory and Compliance	Staff and vendors do not follow the organisation's security policies and processes, leading to non-compliance.				B.2 Policies and procedures B.3 Risk management B.5 Compliance B.6 Audit B.7 Training and awareness										
6	Data Breach	Unauthorised users are abl to access organisation's confidential and/or sensitiv				B.3 Risk management B.8 Assets management B.9 Data protection and										

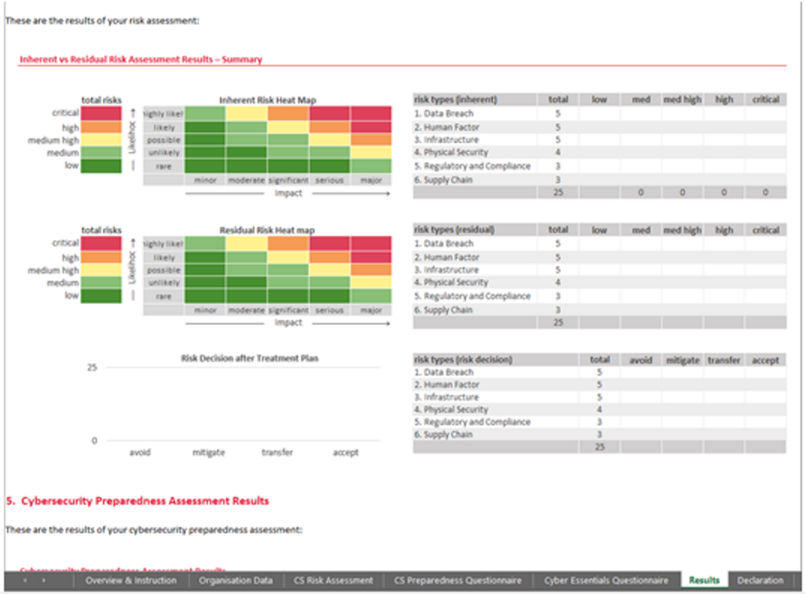
< Back

Next >

Data Security
Cybersecurity Risk Assessment

Cyber Trust Mark

5) Automated heat maps from the inputs to the Risk Assessment worksheet



These are the results of your risk assessment:

Inherent vs Residual Risk Assessment Results – Summary

risk types (inherent)	total	low	med	med high	high	critical
1. Data Breach	5					
2. Human Factor	5					
3. Infrastructure	5					
4. Physical Security	4					
5. Regulatory and Compliance	3					
6. Supply Chain	3					
	25		0	0	0	0

risk types (residual)	total	low	med	med high	high	critical
1. Data Breach	5					
2. Human Factor	5					
3. Infrastructure	5					
4. Physical Security	4					
5. Regulatory and Compliance	3					
6. Supply Chain	3					
	25					

risk types (risk decision)	total	avoid	mitigate	transfer	accept
1. Data Breach	5				
2. Human Factor	5				
3. Infrastructure	5				
4. Physical Security	4				
5. Regulatory and Compliance	3				
6. Supply Chain	3				
	25				

5. Cybersecurity Preparedness Assessment Results

These are the results of your cybersecurity preparedness assessment:

Cybersecurity Preparedness Assessment Results

Data Security
Cybersecurity Risk Assessment

ASEAN
AUSTRALIA
SMART CITIES
TRUST FUND
Asian Development Bank

Cyber Trust Mark

6) Annex provides the Likelihood, Impact and Risk Matrices
7) Also describes the 4 typical risk decisions {Accept, Mitigate, Avoid, Transfer}

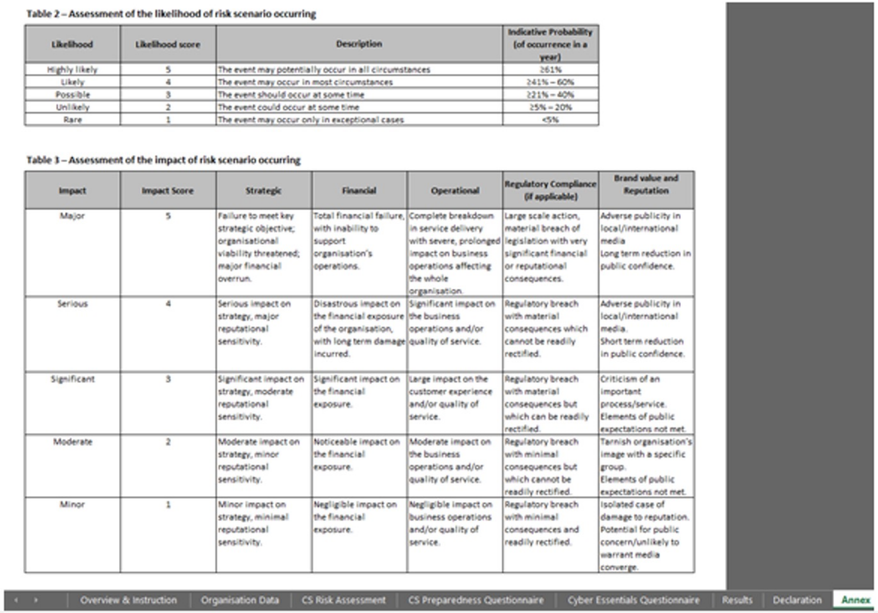


Table 2 – Assessment of the likelihood of risk scenario occurring

Likelihood	Likelihood score	Description	Indicative Probability (of occurrence in a year)
Highly likely	5	The event may potentially occur in all circumstances	≥61%
Likely	4	The event may occur in most circumstances	≥41% – 60%
Possible	3	The event should occur at some time	≥21% – 40%
Unlikely	2	The event could occur at some time	≥5% – 20%
Rare	1	The event may occur only in exceptional cases	<5%

Table 3 – Assessment of the impact of risk scenario occurring

Impact	Impact Score	Strategic	Financial	Operational	Regulatory Compliance (if applicable)	Brand value and Reputation
Major	5	Failure to meet key strategic objective; organisational viability threatened; major financial overrun.	Total financial failure, with inability to support organisation's operations.	Complete breakdown in service delivery with severe, prolonged impact on business operations affecting the whole organisation.	Large scale action, material breach of legislation with very significant financial or reputational consequences.	Adverse publicity in local/international media Long term reduction in public confidence.
Serious	4	Serious impact on strategy, major reputational sensitivity.	Disastrous impact on the financial exposure of the organisation, with long term damage incurred.	Significant impact on the business operations and/or quality of service.	Regulatory breach with material consequences which cannot be readily rectified.	Adverse publicity in local/international media. Short term reduction in public confidence.
Significant	3	Significant impact on strategy, moderate reputational sensitivity.	Significant impact on the financial exposure.	Large impact on the customer experience and/or quality of service.	Regulatory breach with material consequences but which can be readily rectified.	Criticism of an important process/service. Elements of public expectations not met.
Moderate	2	Moderate impact on strategy, minor reputational sensitivity.	Noticeable impact on the financial exposure.	Moderate impact on the business operations and/or quality of service.	Regulatory breach with minimal consequences but which cannot be readily rectified.	Tarnish organisation's image with a specific group. Elements of public expectations not met.
Minor	1	Minor impact on strategy, minimal reputational sensitivity.	Negligible impact on the financial exposure.	Negligible impact on business operations and/or quality of service.	Regulatory breach with minimal consequences and readily rectified.	Isolated case of damage to reputation. Potential for public concern/unlikely to warrant media converge.

< Back

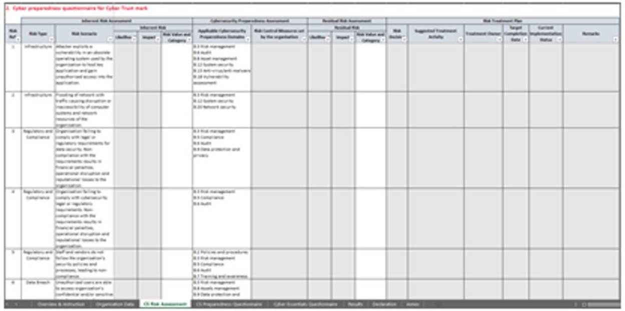
Next >

Data Security
Cybersecurity Risk Assessment

ASEAN AUSTRALIA SMART CITIES TRUST FUND
Asian Development Bank

Smart Livable Cities are Cybersecure Cities

> “Make full use of these valuable but free resources from SG PDPC and CSA to perform Data Protection Impact Assessment (DPIA) for your next data project for your city”



https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-certification-for-organisations/cyber-trust-mark

EXAMPLE

REFLECT & SUBMIT

REQUIRED SUBMISSION

TIME: 30 minutes

REQUIRED MATERIALS: None

Develop Your Own Data Protection Impact Assessment

Overview

Based on home exercise 1 smart city developed use case, it is time to develop a cyber security risk assessment for this use case. This is the final activity for home exercise 2.

STEP 1

Download and open the GLP_Home Exercise_Module2_Cyber Trust Self-Assessment.xlsx. (Excel file download link)
Make sure to "Enable Changes" if Excel asks for this.

STEP 2

Go to the tab "CS Risk Assessment"

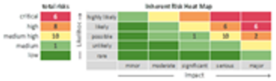
STEP 3

This Cyber Trust risk assessment template is pre-populated with risk scenarios that depict top/common cyber security incidents in **organisations**. Please for this home exercise replace the word "**organsation**" with "**project**" in your mind. For each risk scenario, assess your smart city use case proposal's inherent risk by evaluating the likelihood and impact of the scenarios occurring in your smart city proposal.

Enter a value each for
1) Likelihood (see the tab "Annex" for description of likelihood values)
2) Impact (see the tab "Annex" for description of impact values)

STEP 4

The inherent risk category and value will be automatically computed and the heap map reflecting the smart city project's inherent risk is automatically generated in the tab "Results".

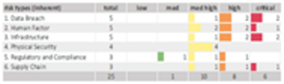


	total risks
critical	6
high	8
medium high	10
medium	1
low	

Inherent Risk Heat Map

Likelihood					
highly likely					
likely				6	6
possible			1	10	2
unlikely					
rare					
	minor	moderate	significant	serious	major

Impact



Risk types (inherent)	total	low	med	med high	high	critical
1. Data Breach	5			1	2	2
2. Human Factor	5			2	2	1
3. Infrastructure	5			1	2	2
4. Physical Security	4			4		
5. Regulatory and Compliance	3		1	1	1	
6. Supply Chain	3			1	1	1
	25		1	10	8	6

< Back   Next >

EXERCISE SUBMISSION

REQUIRED SUBMISSION

Finished with this exercise?

Fill in the information below and follow the steps to submit you/your group's work:

Name of Individual/ Group members: Type your answer here...

City: Type your answer here...

Country: Type your answer here...

STEP 1: Finalize this file by adding your city and last name onto this PPT's file name using the following format:

GLP Exercise 2_[City]_[Your Last Name]
(Example: **GLP Exercise 2_Baguio_Lucero**)

STEP 2: Go to the **GLP Google Drive** and save your renamed file inside the folder named after your city.

NOTE: We also recommend that you also save an offline copy of this file on your computer in case of file syncing issues.

If you encounter any issues with uploading your work, please contact Kristine Lucero of the AASCTF team at kjl@ramboll.com or through WhatsApp or Telegram at +639171702953.

< Back   Next >

Thank you for finalizing Home Exercise 2

Congratulations on finalizing the first home exercise in the ASEAN Australia Smart Cities Trust Fund's Guided Learning Programme on urban data.

Please review your answers in preparation for the group sessions with the Ramboll team (specific date to be advised).

If you have any questions, please reach out to the National Focal Point

Data Collection and Storage

COMPLETED

Data Governance and Security

COMPLETED

Data Analysis and Decision Making

ASEAN AUSTRALIA SMART CITIES TRUST FUND
Asian Development Bank

Australian Government
Department of Foreign Affairs and Trade

ADB