ASEAN AUSTRALIA SMART CITIES TRUST FUND
Asian Development Bank

Australian Government
Department of Foreign Affairs and Trade

ADB

RAMBOLL

Data Protection and Cybersecurity

How to perform a Data Protection Impact Assessment and Cyber Risk Assessment

Wong Onn Chee
CEO
Rajah & Tann Cybersecurity

AASCTF GLP WEBINAR 2:
DATA GOVERNANCE AND SECURITY

Agenda

- A look at SG Personal Data Protection Commission (PDPC) Decisions till 24 Sep 2022
- Data Protection Impact Assessment (DPIA)

  as recommended by SG PDPC
- Cyber Risk Assessment (CRA)

  as recommended by SG Cyber Security Agency (CSA)

PDPC Decisions

1. 173 Decisions for confirmed breaches of PDPA from 2016 till Sep 2022

2. Total penalties: **S$3.073m**

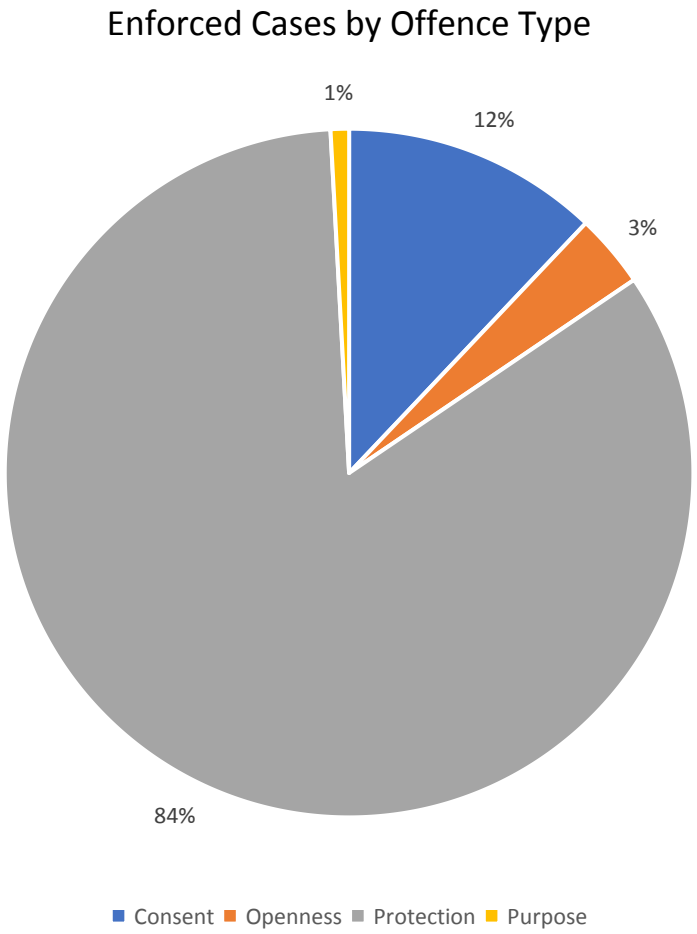
3. Personal data (non-dedup) records: **16.83m**

4. Excluding Singhealth/IHIS case, the next Top 3 offenders by penalties are:
    1. Secure Solutions Group - HSA vendor - leaked blood donor PD - S$120k - 2020
    2. Ninja Logistics - S$90K - 2019
    3. Commeasure (reddoorz.com) - S$74k - 2021

5. All are Breaches of Protection.

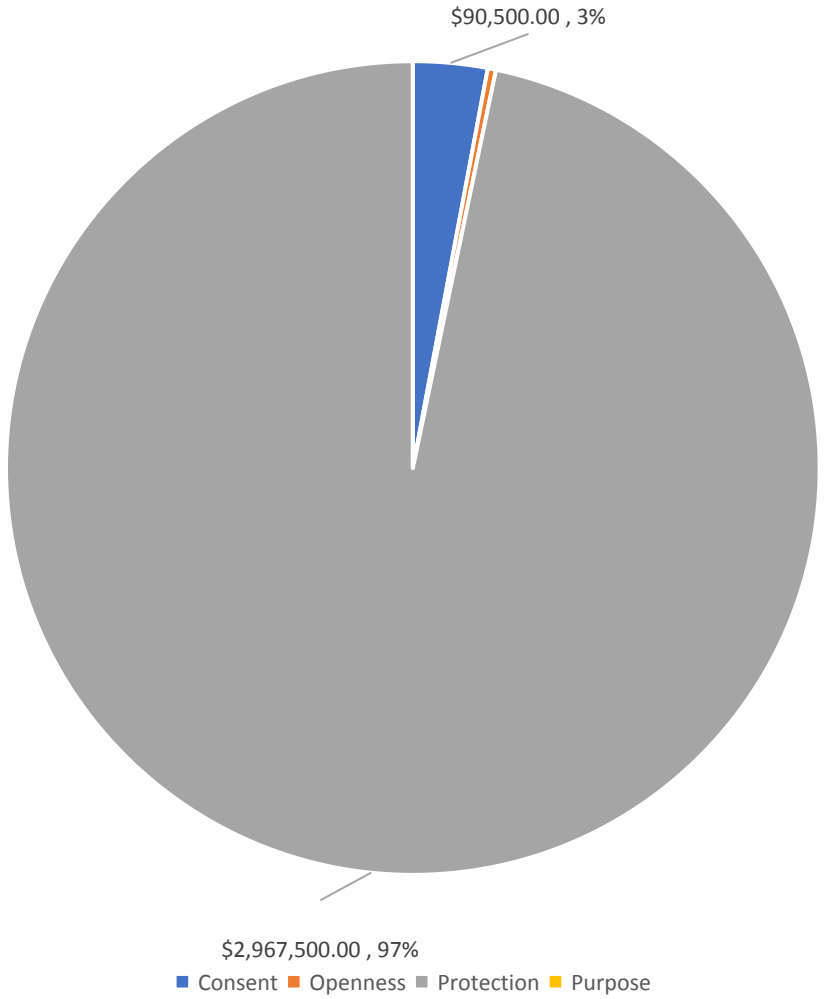
6. In fact, all Top 10 breaches by quantum of penalties are Breaches of Protection.

84% of PDPC Decisions are for Breaches of Protection



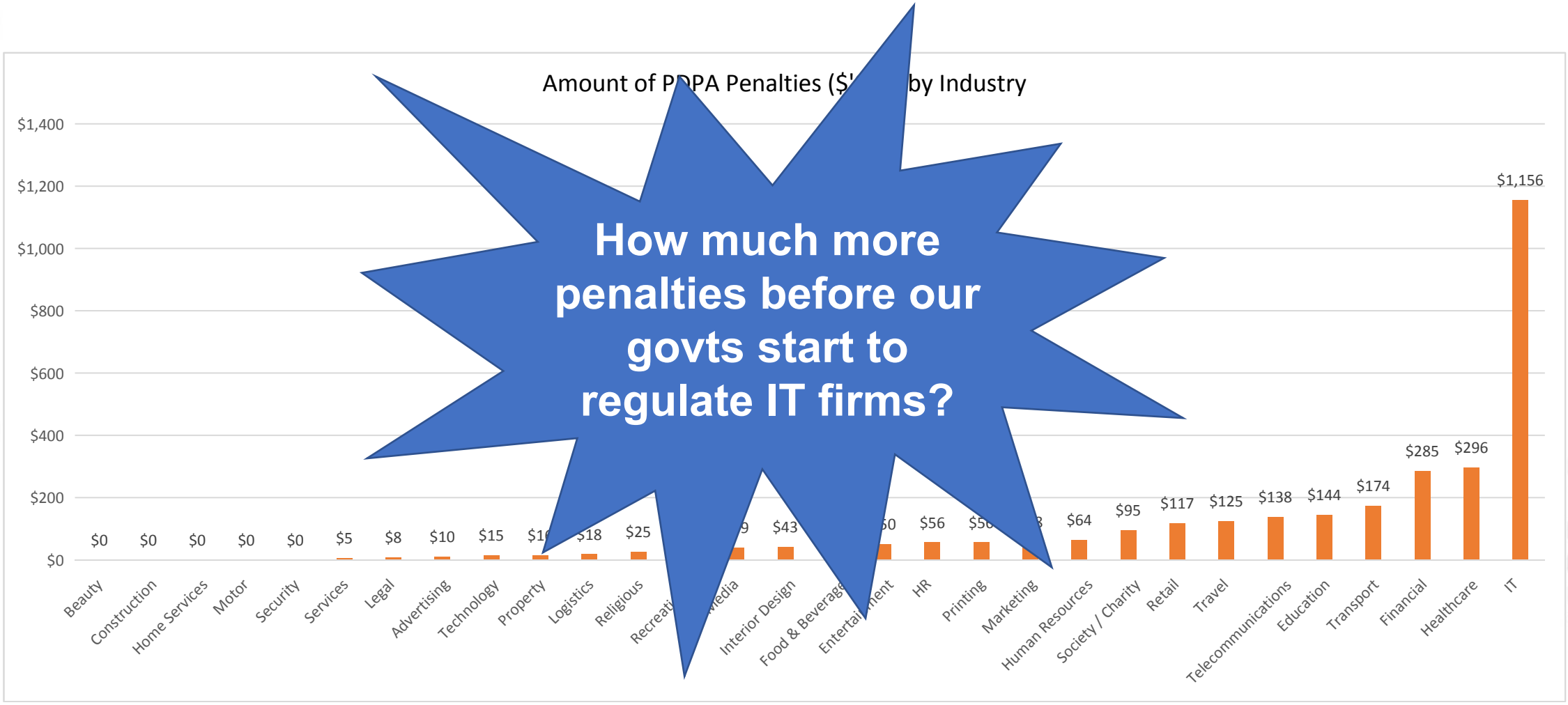
Source: https://www.pdpc.gov.sg/Enforcement-Decisions

97% of PDPA penalties are for Breaches of Protection



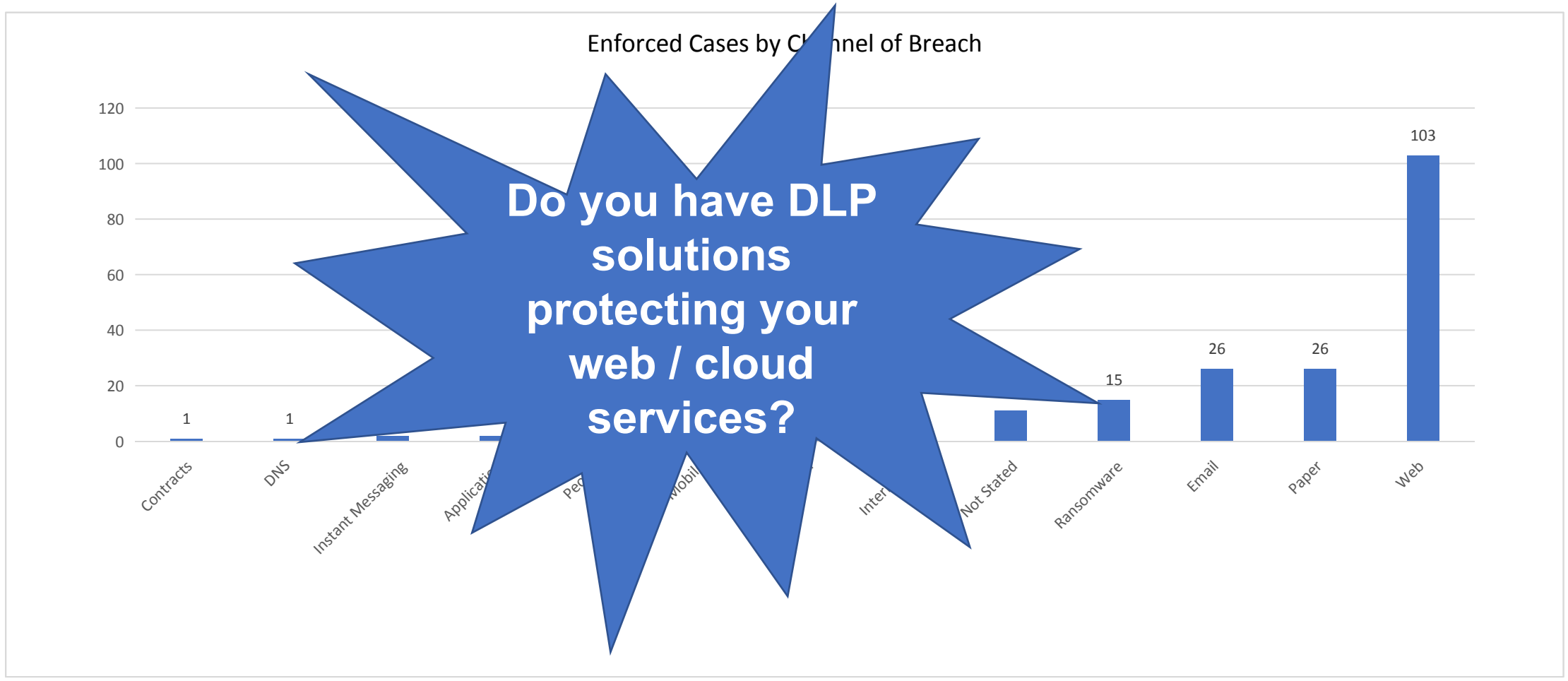
Source: https://www.pdpc.gov.sg/Enforcement-Decisions

IT firms / vendors account for ~S$1.156m of penalties



Source: https://www.pdpc.gov.sg/Enforcement-Decisions

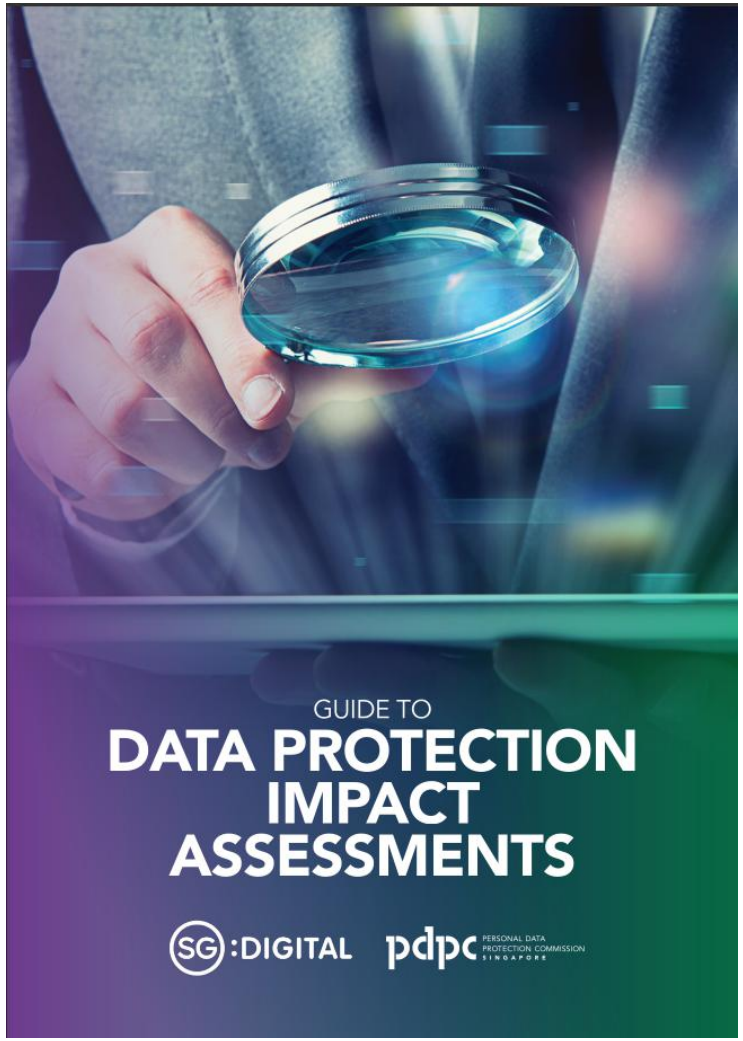
Leakages from web / cloud services are the most common causes



Source: https://www.pdpc.gov.sg/Enforcement-Decisions

Data Protection Impact Assessment

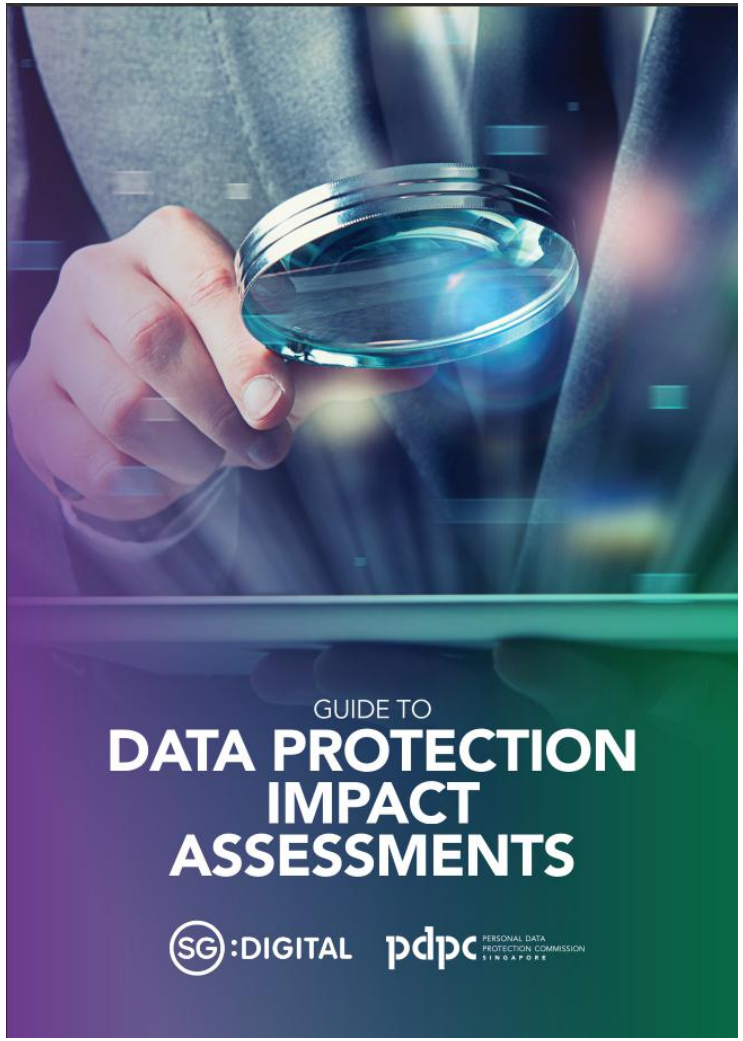
1. Title = “Guide to Data Protection Impact Assessments”
2. Updated in 14 September 2021 to align with the updated SG PDPA (Personal Data Protection Act) which came into force on 1 February 2021.
3. Can be downloaded from https://www.pdpc.gov.sg/help-and-resources/2017/11/guide-to-data-protection-impact-assessments



Data Protection Impact Assessment

1. Covers the 10 principles in SG PDPA.
    1. Consent
    2. Notification
    3. Purpose
    4. Accuracy
    5. Access and Correction
    6. Protection <= where Cybersecurity sits
    7. Retention
    8. Transfer
    9. Data Breach Notification*

    * Unique SG notification thresholds



Data Protection Impact Assessment

- Example DPIA is provided for easy reference

Question	Response and description of evidence/source	What are the personal data risks to individuals?	Risk Rating		
Consent, Notification, Purpose Limitation			Impact	Livelihood	Rating
Is consent obtained from individuals for any collection, use or disclosure of their personal data?	Yes. At point of collection, individuals are notified of the purposes of collecting, using or disclosing their personal data, and will have to select 'I agree' to them in order to submit their electronic registration form. The purposes are also documented in the data protection policy. However, note that the purpose of tracking participants' profiles for future planning is not explicitly disclosed.	As the dataset for tracking participants' profiles will be anonymised for analysis, there is no risk to individuals.	1	1	1

Data Protection Impact Assessment

- Sample DPIA questionnaire is provided in the Annex for reference

ANNEX B: SAMPLE DPIA QUESTIONNAIRE

The questionnaire below illustrates how the DPIA lead can assess the project against a range of PDPA requirements and data protection best practices, and identify gaps or risks related to personal data protection. DPOs can develop or modify the questions based on organisational processes and/or specific project requirements, as well as data protection best practices.

Questions	
Content	
1	Is consent obtained from individuals for any collection, use or disclosure of their personal data?
2	Is personal data being collected directly from individuals? If not, what measures are in place to ensure that the individual had consented or is deemed to have consented to the collection, use or disclosure of their personal data?
3	Is there a process to obtain fresh consent from individuals to use their personal data for a new or different purpose, if applicable?
4	Are individuals able to opt out from providing their personal data, and if so, is this easily understood by individuals?
5	Is there a process for individuals to withdraw their consent for the collection, use or disclosure of their personal data?
6	Are individuals informed of the consequences of withdrawing their consent?

Data Protection Impact Assessment

- Recommend to create an Excel template from the Guide for operational use

Item	Questions	Response and description of evidence/source	What are the personal data risks to individuals?	Risk Rating		
				Impact	Livelihood	Rating
Consent						
1	Is consent obtained from individuals for any collection, use or disclosure of their personal data?					
2	Is personal data being collected directly from individuals? If not, what measures are in place to ensure that the individual had consented or is deemed to have consented to the collection, use or disclosure of their personal data?					
3	Is there a process to obtain fresh consent from individuals to use their personal data for a new or different purpose, if applicable?					
4	Are individuals able to opt out from providing their personal data, and if so, is this easily understood by individuals?					
5	Is there a process for individuals to withdraw their consent for the collection, use or disclosure of their personal data?					
6	Are individuals informed of the consequences of withdrawing their consent?					
Notification						
7	Are individuals notified of the purposes of collecting, using or disclosing of their personal data?					

Cybersecurity Risk Assessment

Cyber Trust Mark

The **Cyber Trust** mark is a cybersecurity certification for organisations with more extensive digitalised business operations. It serves as a mark of distinction for your organisation to prove that you have put in place good cybersecurity practices and measures that are commensurate with your cybersecurity risk profile.

Why should my organisation apply?

- Signifies a mark of distinction to recognise organisations as trusted partners with robust cybersecurity
- Provides 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

Demonstrate that you are a trusted business partner.

Scan to learn more:

Which tier of Cybersecurity Preparedness does my organisation belong to?

There are five Cybersecurity Preparedness tiers, with 10 to 22 domains under each tier. Organisations can use the Cyber Trust mark risk assessment framework to identify which Cybersecurity Preparedness tier is more suitable for their needs.

	Tier 1: Supporter	Tier 2: Practitioner	Tier 3: Promoter	Tier 4: Performer	Tier 5: Advocate
Cyber Governance and Oversight					
1. Governance			•	•	•
2. Policies and procedures			•	•	•
3. Risk management	•	•	•	•	•
4. Cyber strategy					•
5. Compliance	•	•	•	•	•
6. Audit				•	•
Cyber Education					
7. Training and awareness*	•	•	•	•	•
Information Asset Protection					
8. Asset management*	•	•	•	•	•
9. Data protection and privacy*	•	•	•	•	•
10. Backups*	•	•	•	•	•
11. Bring Your Own Device (BYOD)				•	•
12. System security*	•	•	•	•	•
13. Anti-virus/Anti-malware*	•	•	•	•	•
14. Secure Software Development Life Cycle (SDLC)					•
Secure Access and Environment					
15. Access control*	•	•	•	•	•
16. Cyber threat management				•	•
17. Third-party risk and oversight					•
18. Vulnerability assessment			•	•	•
19. Physical/environmental security		•	•	•	•
20. Network security		•	•	•	•
Cybersecurity Resilience					
21. Incident response*	•	•	•	•	•
22. Business continuity/disaster recovery		•	•	•	•
	10 DOMAINS	13 DOMAINS	16 DOMAINS	19 DOMAINS	22 DOMAINS

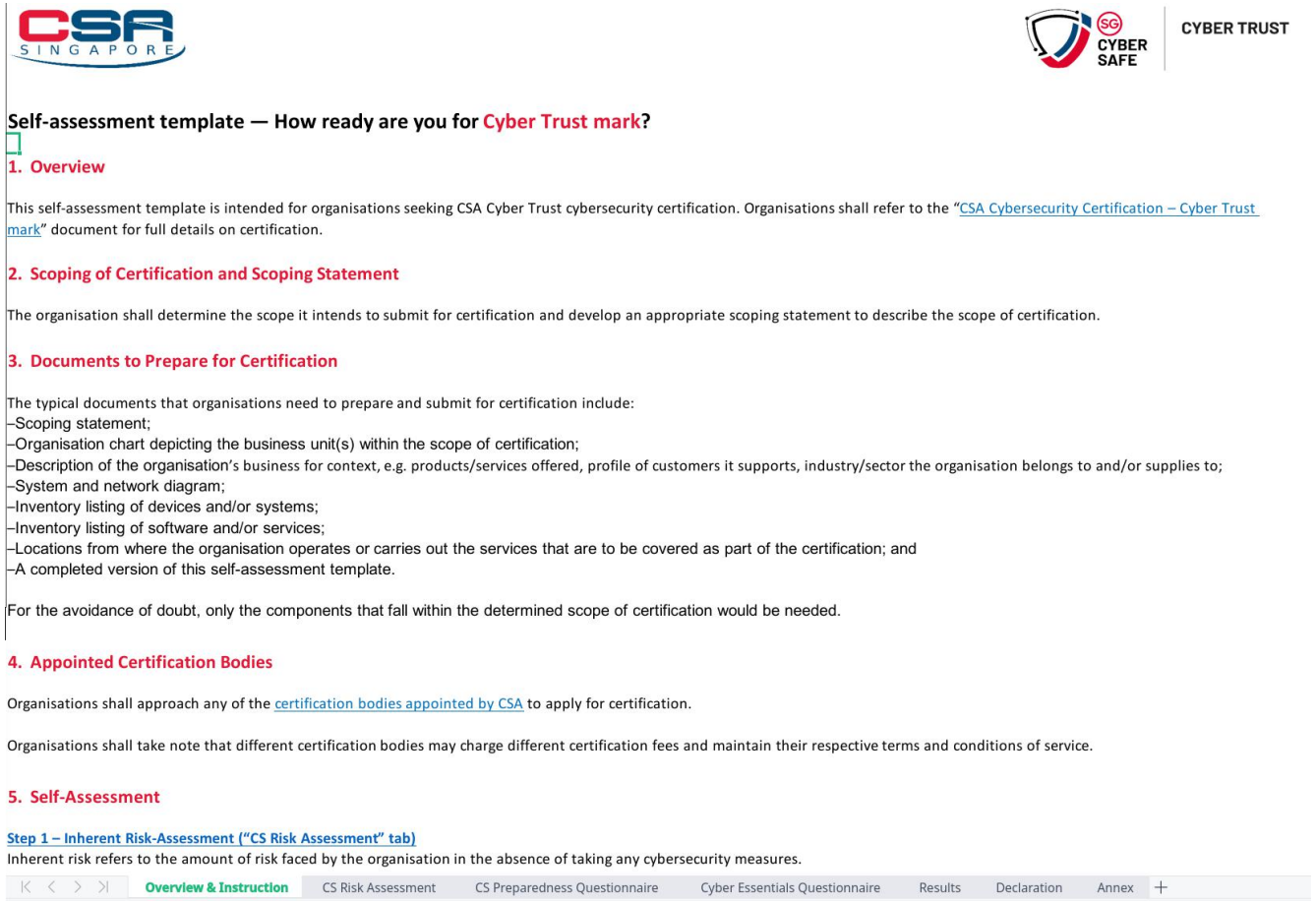
*Measures in Cyber Essentials mark

CSA SINGAPORE

SG CYBER SAFE | CYBER TRUST

1. SG Cyber Trust Mark
2. Comes with SG Cyber Essentials Mark
3. Released on 29 March 2022
4. Can be downloaded from https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-certification-for-organisations/cyber-trust-mark

Cybersecurity Risk Assessment



Self-assessment template — How ready are you for Cyber Trust mark?

1. Overview

This self-assessment template is intended for organisations seeking CSA Cyber Trust cybersecurity certification. Organisations shall refer to the "CSA Cybersecurity Certification – Cyber Trust mark" document for full details on certification.

2. Scoping of Certification and Scoping Statement

The organisation shall determine the scope it intends to submit for certification and develop an appropriate scoping statement to describe the scope of certification.

3. Documents to Prepare for Certification

The typical documents that organisations need to prepare and submit for certification include:
–Scoping statement;
–Organisation chart depicting the business unit(s) within the scope of certification;
–Description of the organisation's business for context, e.g. products/services offered, profile of customers it supports, industry/sector the organisation belongs to and/or supplies to;
–System and network diagram;
–Inventory listing of devices and/or systems;
–Inventory listing of software and/or services;
–Locations from where the organisation operates or carries out the services that are to be covered as part of the certification; and
–A completed version of this self-assessment template.

For the avoidance of doubt, only the components that fall within the determined scope of certification would be needed.

4. Appointed Certification Bodies

Organisations shall approach any of the certification bodies appointed by CSA to apply for certification.

Organisations shall take note that different certification bodies may charge different certification fees and maintain their respective terms and conditions of service.

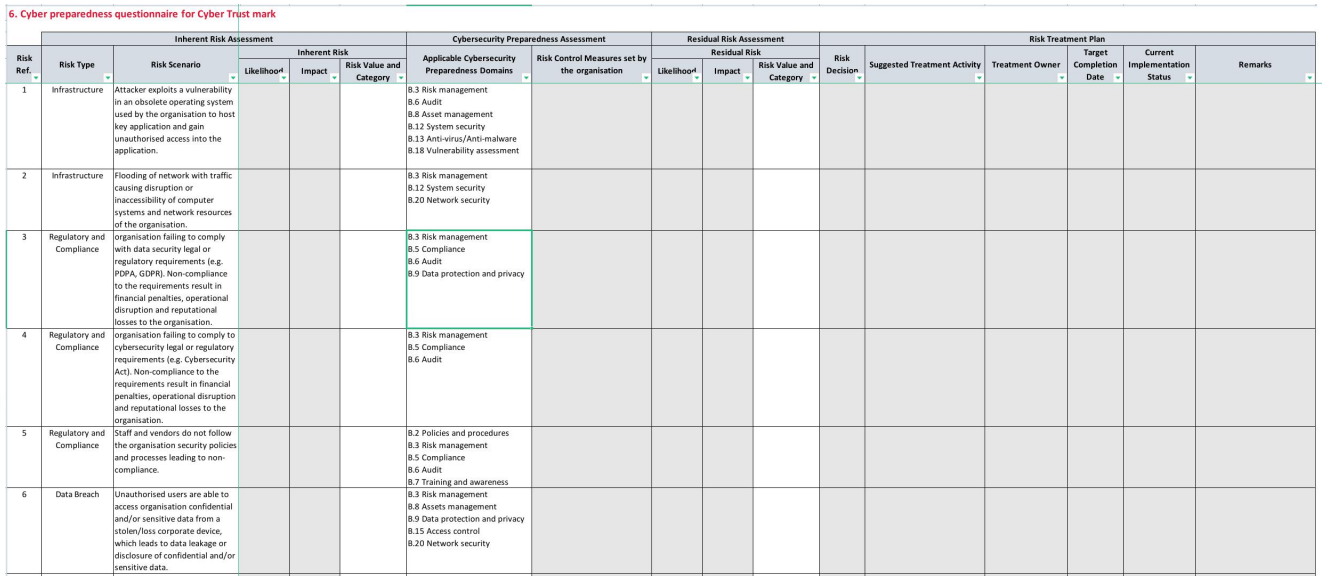
5. Self-Assessment

Step 1 – Inherent Risk-Assessment ("CS Risk Assessment" tab)
Inherent risk refers to the amount of risk faced by the organisation in the absence of taking any cybersecurity measures.

Overview & Instruction | CS Risk Assessment | CS Preparedness Questionnaire | Cyber Essentials Questionnaire | Results | Declaration | Annex

1. Comes with a recommended risk assessment template "CS Risk Assessment" in the Self-Assessment Excel template.

Cybersecurity Risk Assessment



6. 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	Likelihood	Impact	Risk Value and Category	Applicable Cybersecurity Preparedness Domains	Risk Control Measures set by the organisation	Likelihood	Impact	Risk Value and Category	Risk Decision	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 the organisation to host key application and gain unauthorised access into the 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 or 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 data security legal or regulatory requirements (e.g. PDPA, GDPR). Non-compliance to the requirements result 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 to cybersecurity legal or regulatory requirements (e.g. Cybersecurity Act). Non-compliance to the requirements result 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 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 able to access organisation confidential and/or sensitive data from a stolen/loss corporate device, which leads to data leakage or disclosure of confidential and/or sensitive data.				B.3 Risk management B.8 Assets management B.9 Data protection and privacy B.15 Access control B.20 Network security											

1. 25 key cyber risks to assess.
2. 6 types of cyber risks
    1. Data Breach (5)
    2. Human Factor (5)
    3. Infrastructure (5)
    4. Physical Security (4)
    5. Regulatory and Compliance (3)
    6. Supply Chain (3)

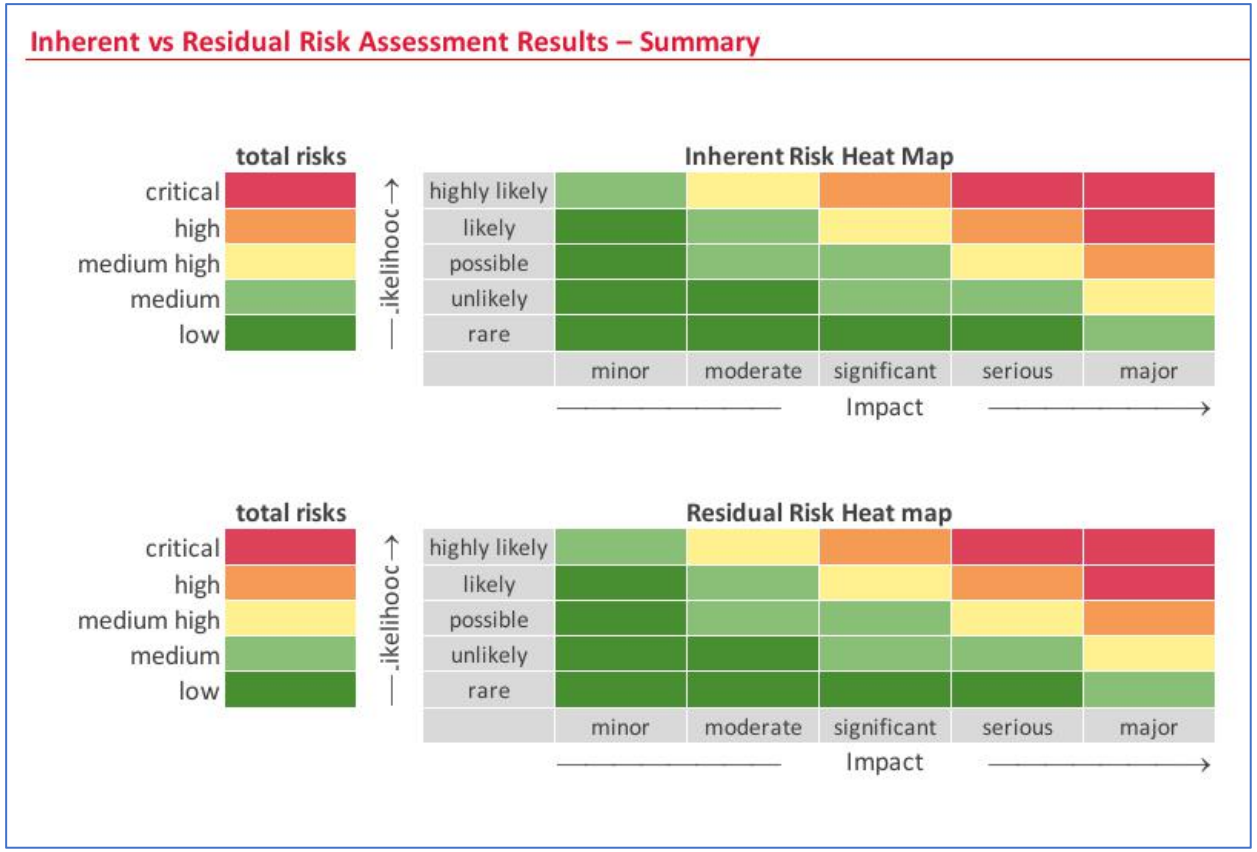
Cybersecurity Risk Assessment

6. 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	Likelihood	Impact	Risk Value and Category	Applicable Cybersecurity Preparedness Domains	Risk Control Measures set by the organisation	Likelihood	Impact	Risk Value and Category	Risk Decision	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 the organisation to host key application and gain unauthorised access into the 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 or 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 data security legal or regulatory requirements (e.g. PDPA, GDPR). Non-compliance to the requirements result 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 to cybersecurity legal or regulatory requirements (e.g. Cybersecurity Act). Non-compliance to the requirements result 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 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 able to access organisation confidential and/or sensitive data from a stolen/loss corporate device, which leads to data leakage or disclosure of confidential and/or sensitive data.				B.3 Risk management B.8 Assets management B.9 Data protection and privacy B.15 Access control B.20 Network security											

3. Look at Inherent Risks and Residual Risks after identifying Risk Control Measures across 22 domains.
4. Includes Risk Treatment Plan so that projects can plan, budget and implement additional controls to lower the risks.

Cybersecurity Risk Assessment



5. Generates automated heat maps from the inputs to the Risk Assessment worksheet.

Cybersecurity Risk Assessment

Annex: Risk Assessment Terminologies and Definitions

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 will occur in most circumstances.	≥61%
Likely	4	The event shall probably 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 but 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.

6. Annex provides the Likelihood, Impact and Risk Matrices.

7. Also describes the 4 typical Risk Decisions
   1. Accept
   2. Mitigate
   3. Avoid
   4. Transfer

Conclusions

- Make full use of these 2 valuable but free resources from SG PDPC and CSA to perform DPIA and CRA for your next data project for your city.

- Remember the wise adages:
  - What you can't measure, you can't manage
  - What you don't manage, you will lose

- Don't be the next victim of data breach.

ASEAN AUSTRALIA SMART CITIES TRUST FUND
Asian Development Bank

Australian Government
Department of Foreign Affairs and Trade

ADB

RAMBOLL

Thank you!

Wong Onn Chee

onnchee@rtcyber.com