Leadership in Enterprise Risk Management

22 October 2021

Business Continuity • **Enterprise Risk** • **Disaster Recovery** • **Crisis Management**

BCP ASIA®

Preparing Business. Enhancing Minds

Consultancy • Training • Internal Audit • Software

Henry Ee *FBCI, CBCP, ACTA, ISO22301 Auditor*

Technical Expert (Business Continuity / Resilience),
ISO - International Organization for Standardization

More than 20 years of experience in Risk, Resilience, Business Continuity & Crisis Management

CREDENTIALS

- Chairman, Business Continuity Institute Asia Chapter
- Vice President, RIMAS
- ISO 22301 Working Group Member, Singapore Standard Development
- Certified Management Consultant, PMC
- Chairman, IAEM (US) SE Asia Chapter
- Certified ISO22301 Lead Auditor (ANSI)
- ISO 31000 Certified Lead Risk Manager, PECB
- Certified Trainer (ACTA) by WDA Singapore
- Approved Trainer by BCI, PECB, EXIN
- Member of UNDRR, Private-Public Partnership for Disaster Management

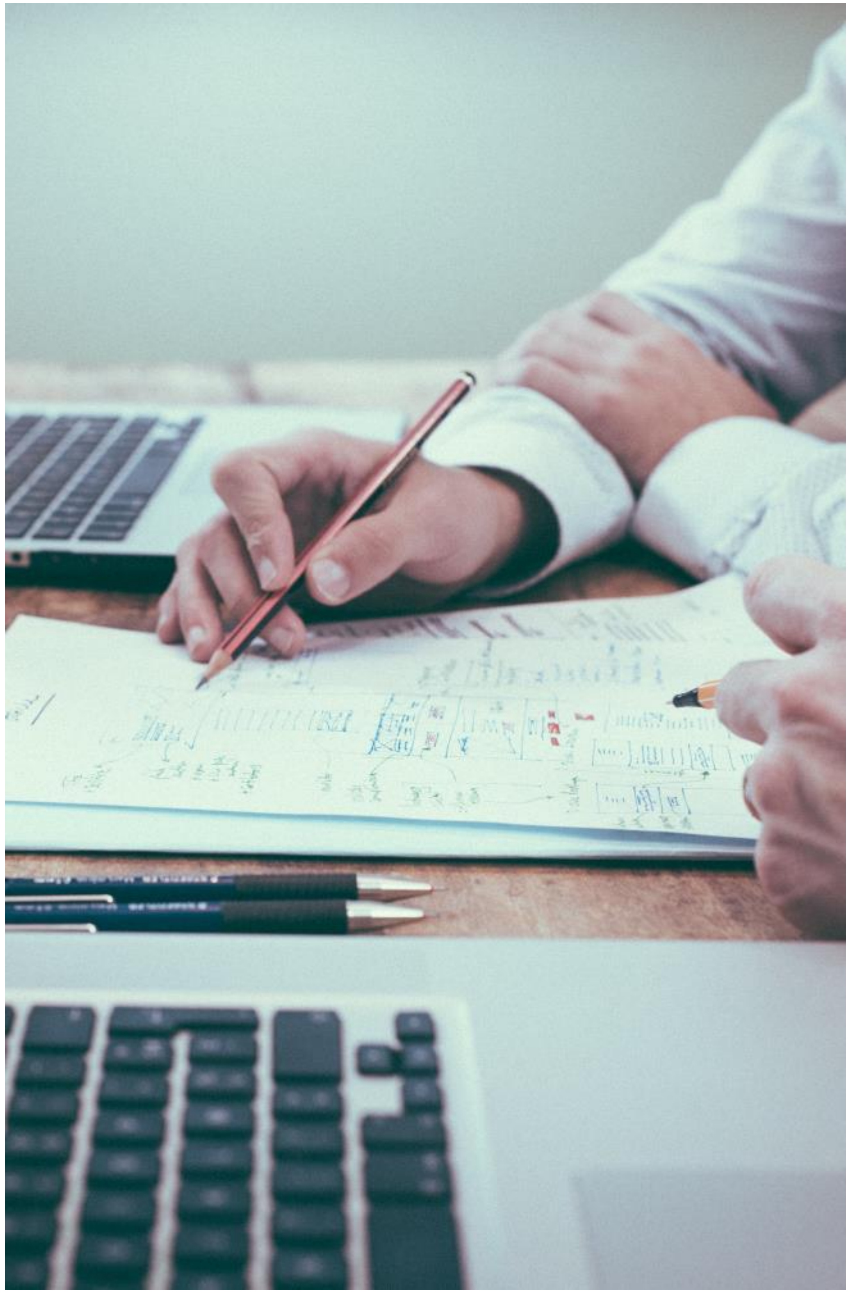
Pre-Training Questionnaire

Your inputs are valuable to us, please spend **8 minutes** to answer the pre-training questionnaire and submit it before the training starts.

bit.ly/pre1022

Agenda

1. Introduction to Risk Management
2. Policy & Risk Governance Structure
3. Risk Management Processes
4. What’s Next?



Introduction to Risk Management

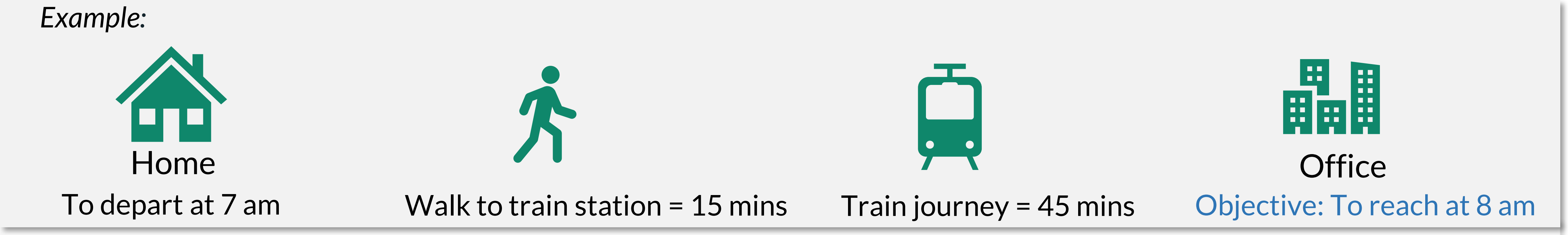
What is Risk?

Effect of uncertainty on objectives.

Effect - An effect is a deviation from the expected. *(ISO31000:2018)*

Event can be an Incident (usually negative) or something that has not happened (positive or negative).

Example:



Event - Faulty alarm / water shortage / power outage in the morning

Event - Road repair work / raining

Event - Train delay due to signalling fault

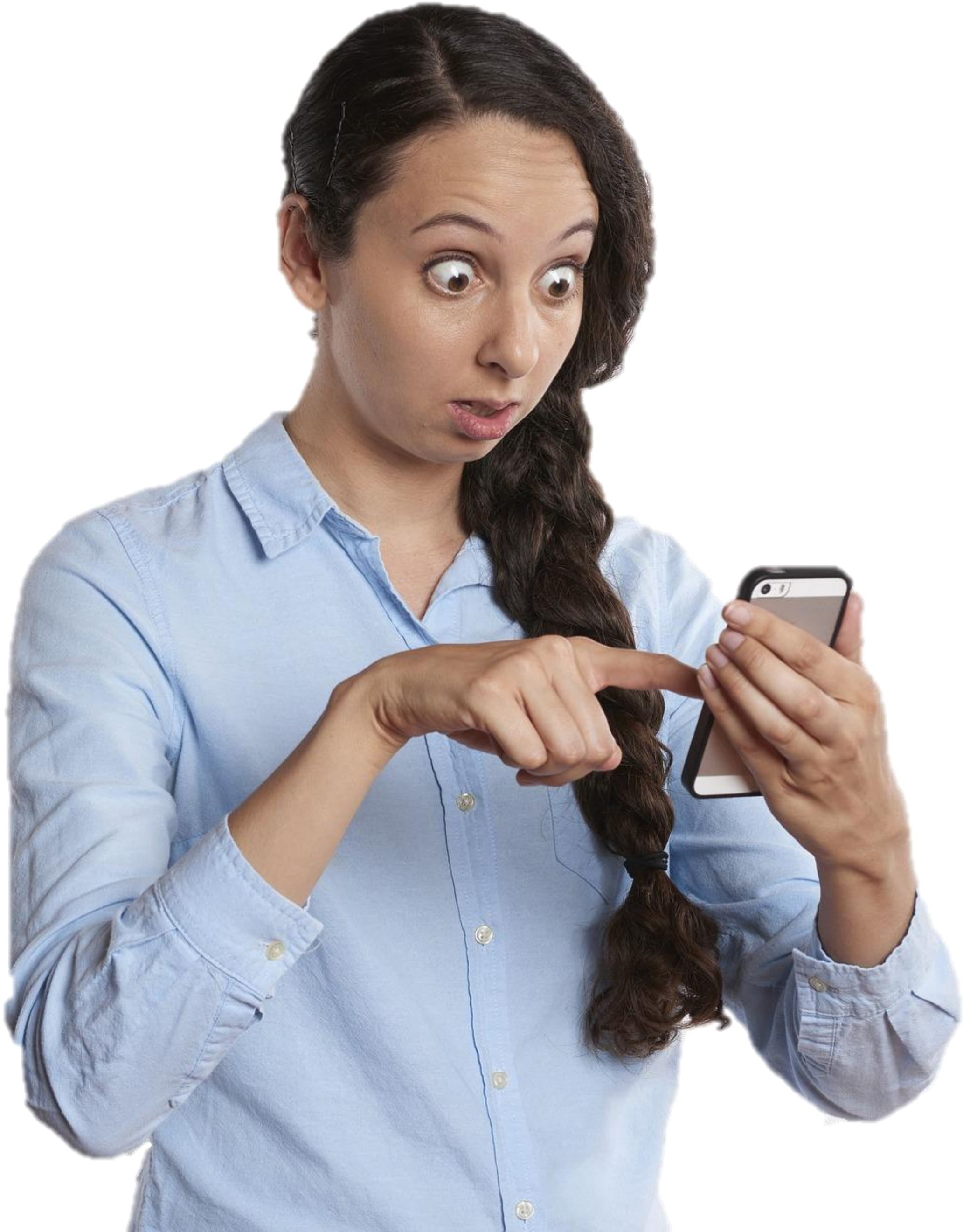
Uncertainties: Will he be able to wake up / get ready on time?

Uncertainties: Will he be able to walk from his house to train station within 15 minutes?

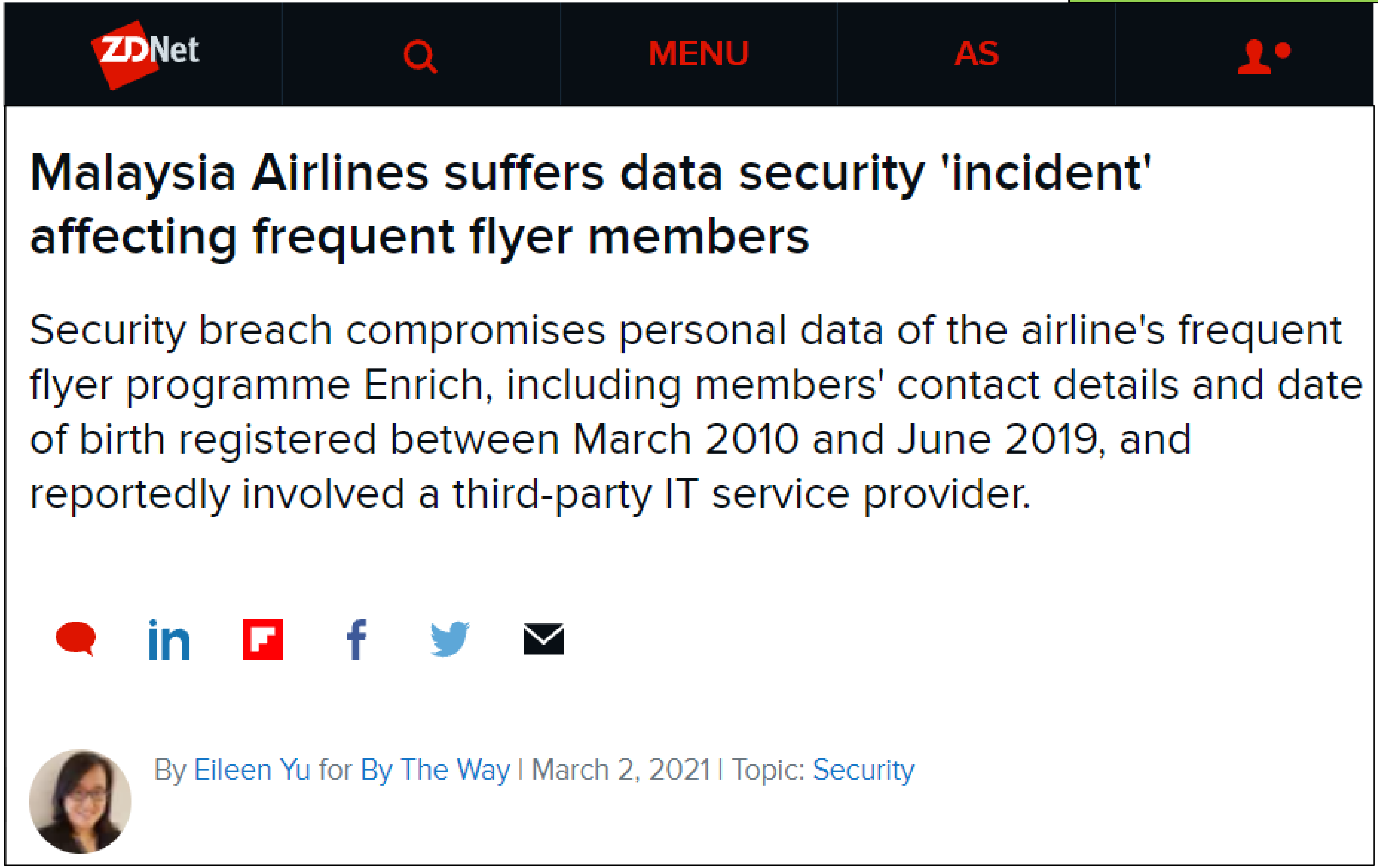
Uncertainties: Will he able get on train on time?

Effect: Late for 10 minutes

WHAT IS HAPPENING AROUND US?



March 2021 (Malaysia)

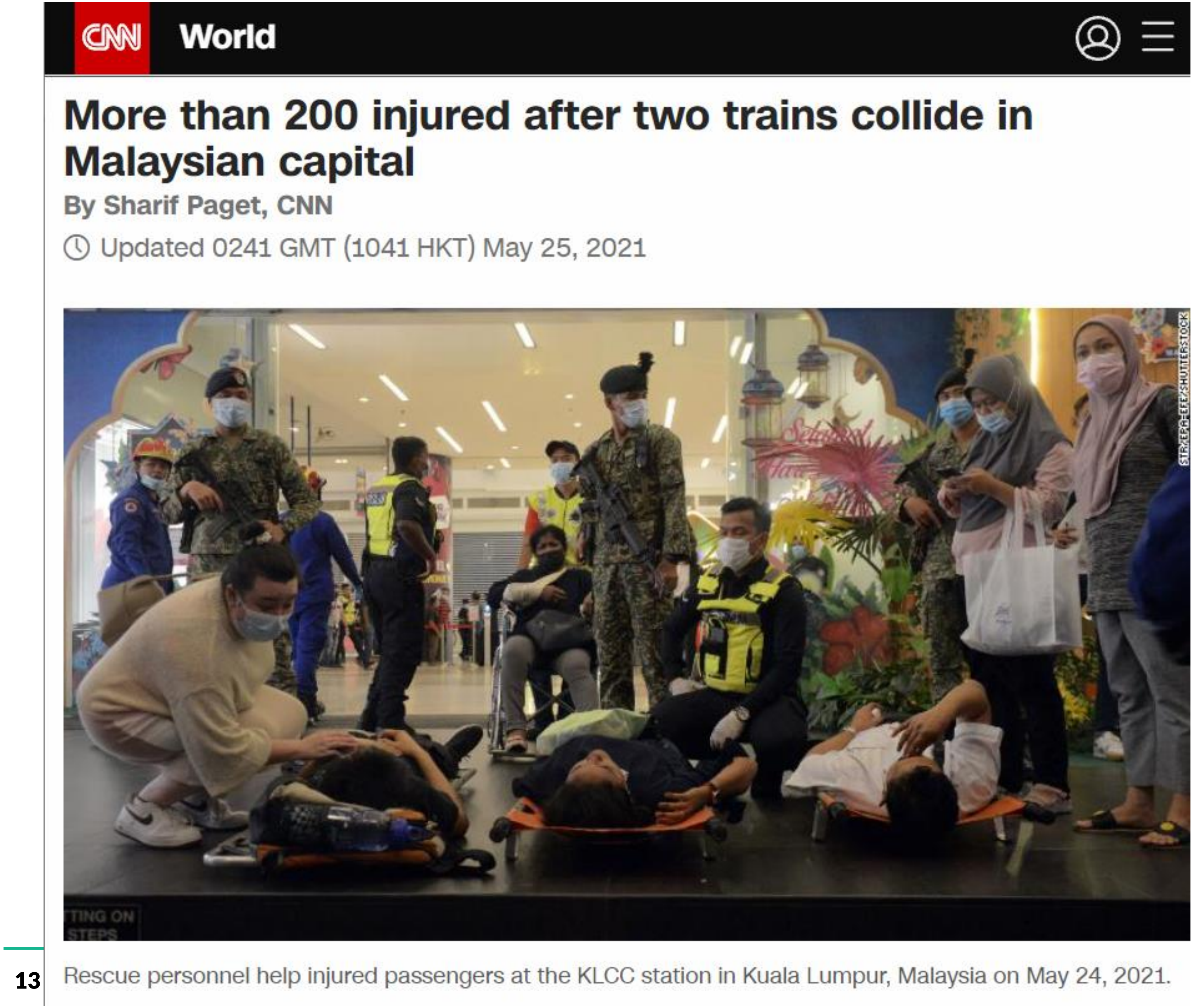


Malaysia Airlines suffers data security 'incident' affecting frequent flyer members

Security breach compromises personal data of the airline's frequent flyer programme Enrich, including members' contact details and date of birth registered between March 2010 and June 2019, and reportedly involved a third-party IT service provider.

By Eileen Yu for By The Way | March 2, 2021 | Topic: Security

May 2021 (Malaysia)



More than 200 injured after two trains collide in Malaysian capital

By Sharif Paget, CNN

Updated 0241 GMT (1041 HKT) May 25, 2021

Rescue personnel help injured passengers at the KLCC station in Kuala Lumpur, Malaysia on May 24, 2021.

SingHealth Cyber Attack

July 2018 (Singapore)

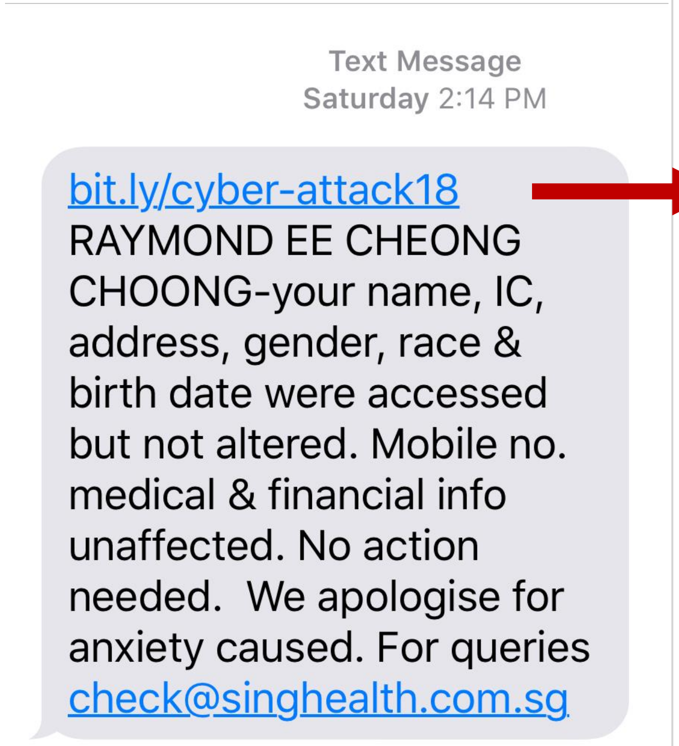
The Victims of Singapore’s Largest Data Breach

1.5 Million Patients

PM Lee

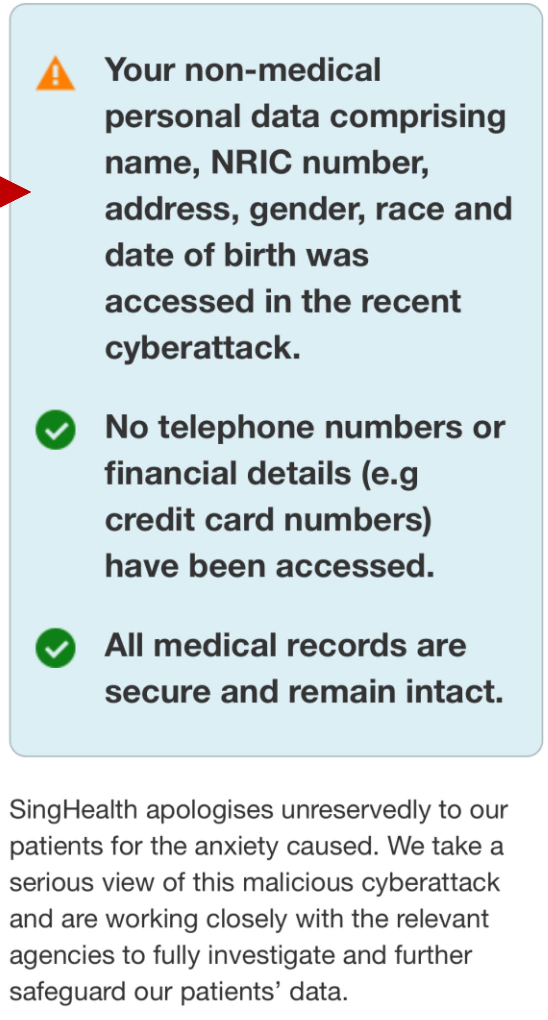
Other Ministers

SingHealth Cyber Attack



Text Message
Saturday 2:14 PM

bit.ly/cyber-attack18 RAYMOND EE CHEONG CHOONG-your name, IC, address, gender, race & birth date were accessed but not altered. Mobile no. medical & financial info unaffected. No action needed. We apologise for anxiety caused. For queries check@singhealth.com.sg

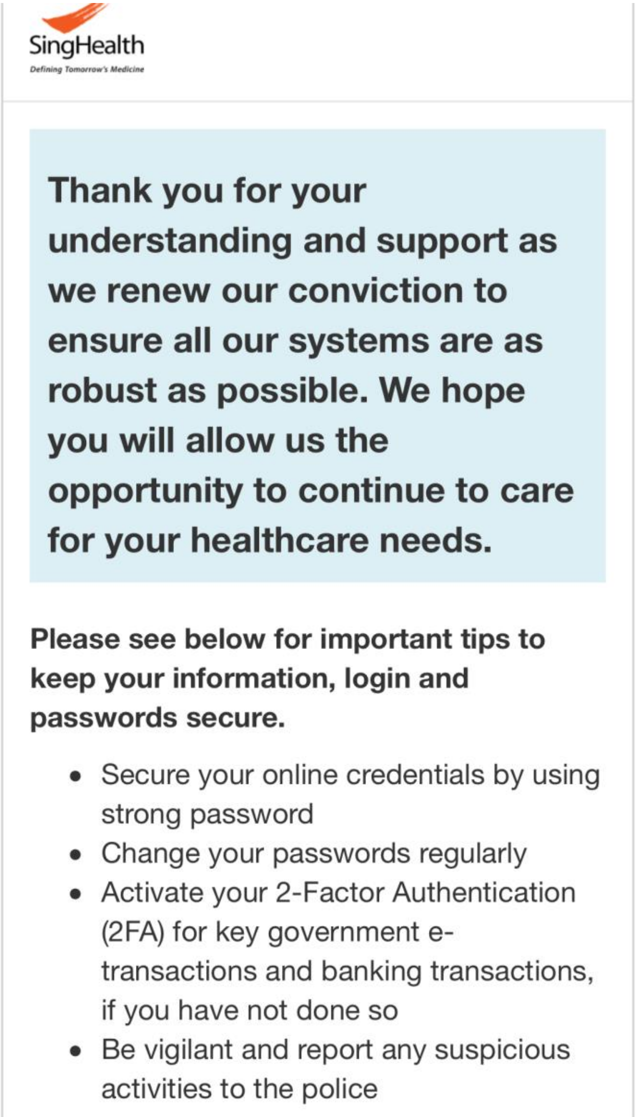


⚠ Your non-medical personal data comprising name, NRIC number, address, gender, race and date of birth was accessed in the recent cyberattack.

✓ No telephone numbers or financial details (e.g credit card numbers) have been accessed.

✓ All medical records are secure and remain intact.

SingHealth apologises unreservedly to our patients for the anxiety caused. We take a serious view of this malicious cyberattack and are working closely with the relevant agencies to fully investigate and further safeguard our patients' data.



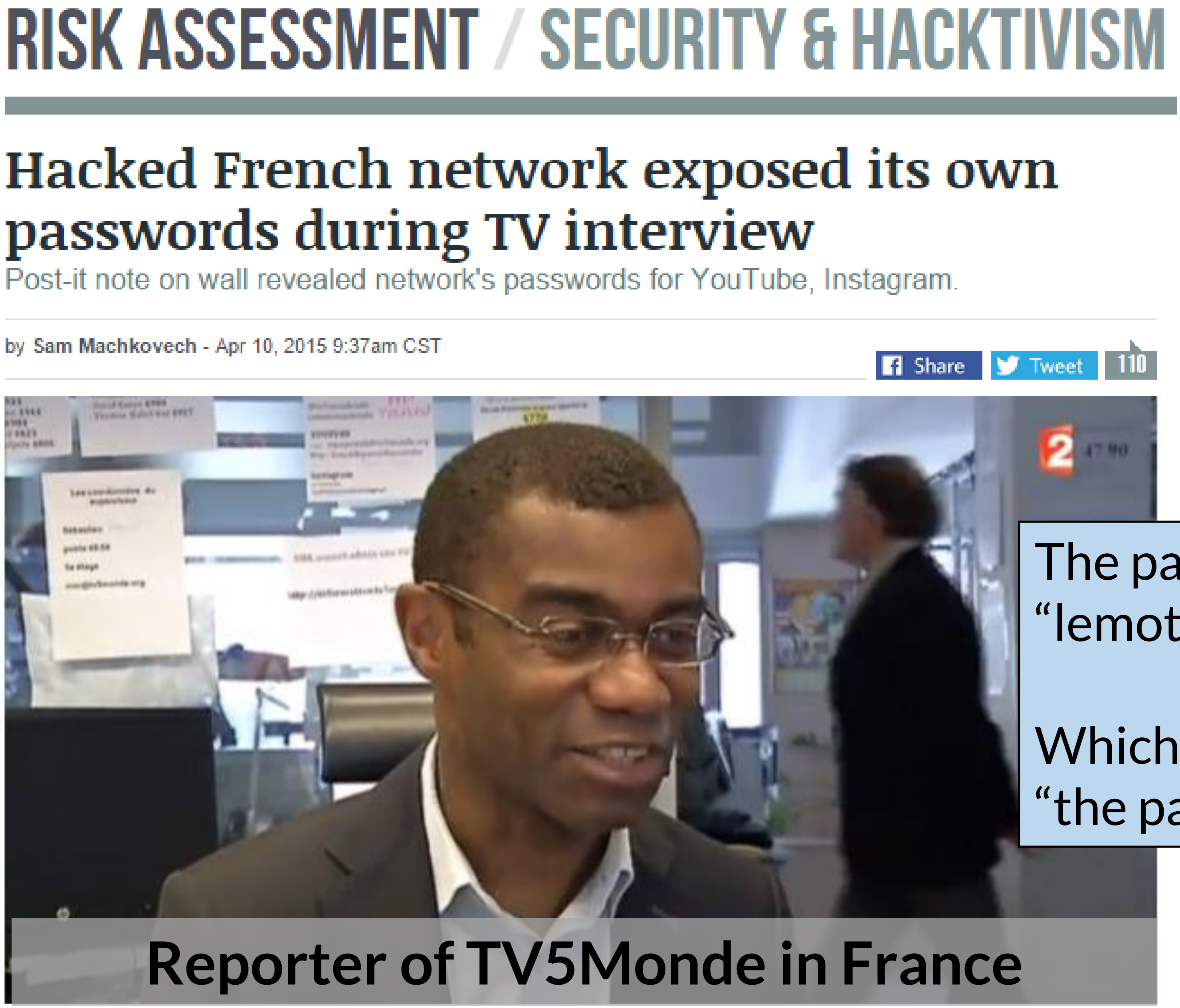
SingHealth
Defining Tomorrow's Medicine

Thank you for your understanding and support as we renew our conviction to ensure all our systems are as robust as possible. We hope you will allow us the opportunity to continue to care for your healthcare needs.

Please see below for important tips to keep your information, login and passwords secure.

- Secure your online credentials by using strong password
- Change your passwords regularly
- Activate your 2-Factor Authentication (2FA) for key government e-transactions and banking transactions, if you have not done so
- Be vigilant and report any suspicious activities to the police

April 2015 (France)



RISK ASSESSMENT / SECURITY & HACKTIVISM

Hacked French network exposed its own passwords during TV interview

Post-it note on wall revealed network's passwords for YouTube, Instagram.

by Sam Machkovech - Apr 10, 2015 9:37am CST

Reporter of TV5Monde in France

The password is: “lemotdepassedeyoutube,”

Which translates to English: “the password of youtube”

How could Risk Management help?

Risk Assessment

- Conduct **ongoing risk assessments** to **scan for potential weak points**.

Direct Investment

- **Direct** investments based on the findings of risk assessments, e.g. **strengthen the vulnerability management, network monitoring and threat intelligence**.

Risk Treatment

- **Prioritize** the efforts in risk treatment (reduce the likelihood of incident & reduce the impact). Focus on the projects which could greatly reduce the risk.

Ownership

- Assign **ownership** to identify, mitigate and monitor the risks, e.g. risk champions / risk owners / control owners.

Communication

- **Communicate** with the relevant stakeholders to foster teamwork and mutual accountability among all parties.

Activity

"Even if an organisation is prepared to accept the consequences, its **stakeholders** may not."

In your view, who is MCMC's major ERM stakeholder?

A. Employees

B. Customers

C. Government

D. Others:__________

Activity

What risk management means to MCMC?

A. Drive profitability & minimize big losses

B. Maintain a good reputation

C. Ensure regulatory compliance

D. Protect the stakeholders

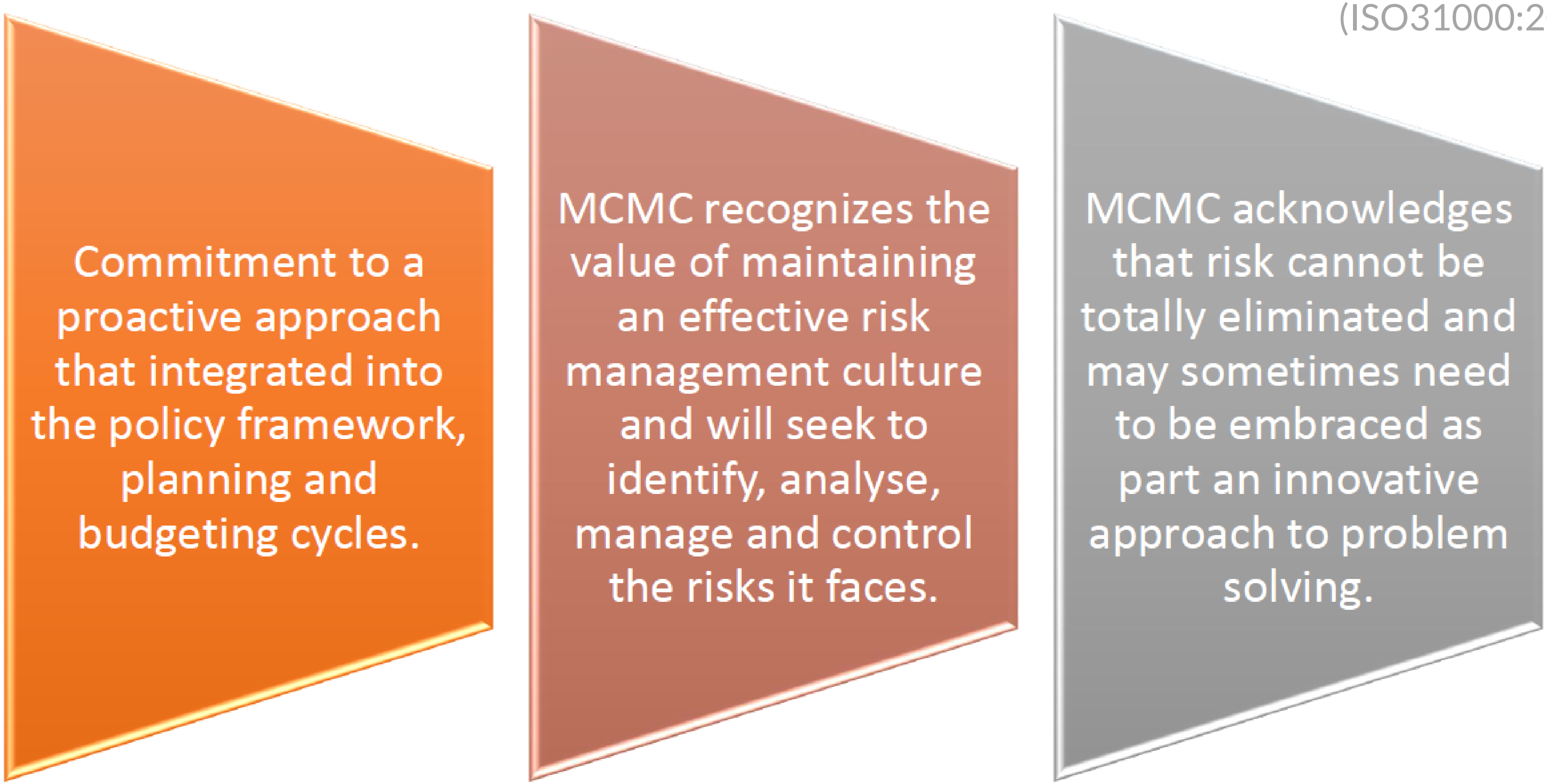
E. Others:___________

MCMC Risk Management Policy & Risk Governance Structure

ERM Policy Statement

Policy: A Statement of the overall intentions and direction of an organization related to Risk Management.

(ISO31000:2018)

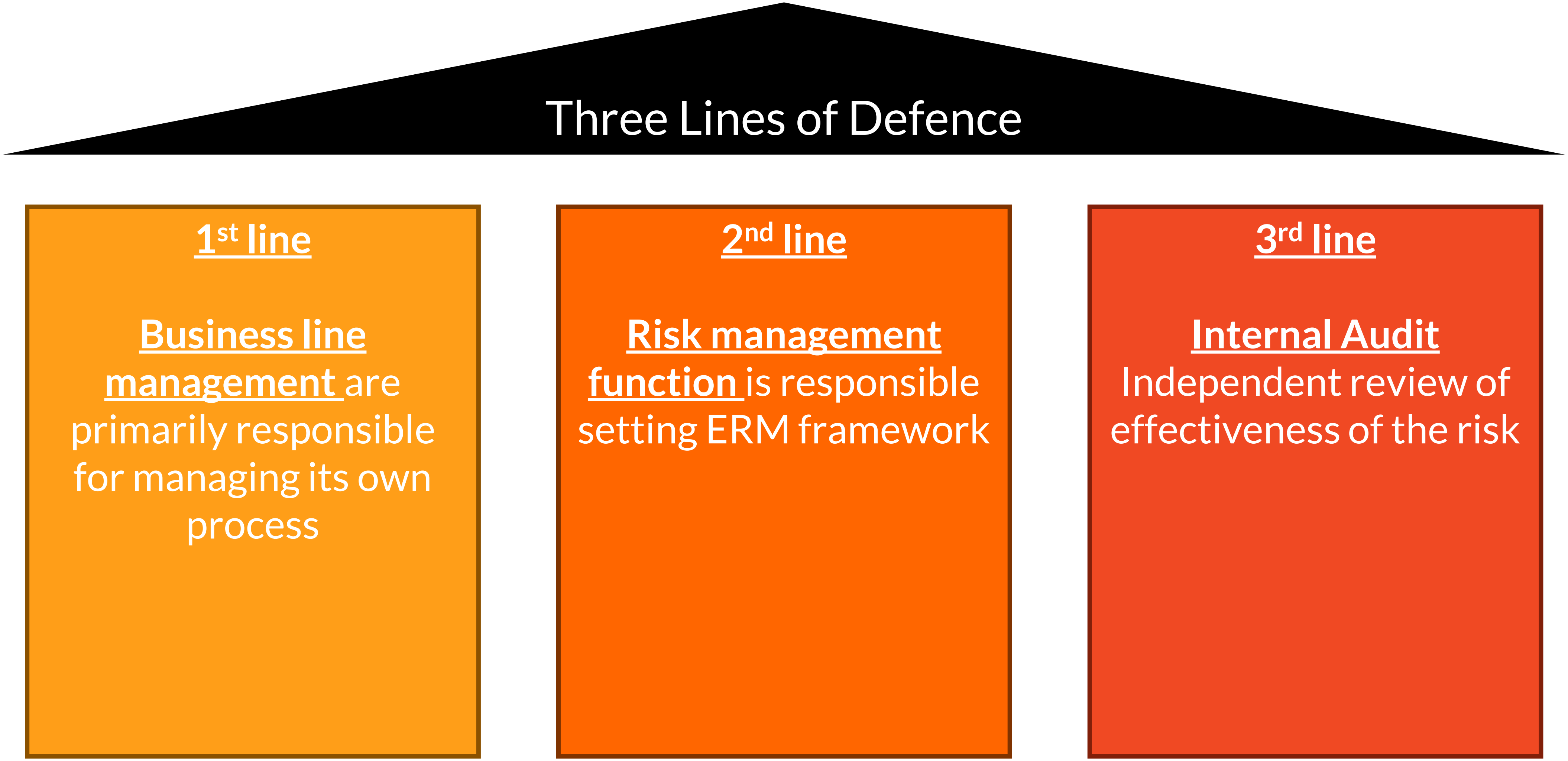


Commitment to a proactive approach that integrated into the policy framework, planning and budgeting cycles.

MCMC recognizes the value of maintaining an effective risk management culture and will seek to identify, analyse, manage and control the risks it faces.

MCMC acknowledges that risk cannot be totally eliminated and may sometimes need to be embraced as part an innovative approach to problem solving.

Risk Governance



Three Lines of Defence

1st line

Business line management are primarily responsible for managing its own process

2nd line

Risk management function is responsible setting ERM framework

3rd line

Internal Audit Independent review of effectiveness of the risk

Risk Governance

Three Lines of Defence

1st line

Business line management are primarily responsible for managing its own process

- **Risk Champions (Head of Department / Division):** Assess, control and monitor the risks with the aim of achieving downside protection against negative surprises, and maximizing upside potential when opportunities arise
- **Control Owner:** Update the relevant policies, procedures and controls to manage the risks in the Risk Registers

Risk Governance

Three Lines of Defence

2nd line

Risk management function is responsible setting ERM framework

- Risk Management Department: Act as a central control and guide for risk management issues within the organization; Supervise risk management implementation at the organization level;
- Risk Committee (Management): Provide oversight of the risk management system, set risk management policies and guidelines.

Risk Governance

Three Lines of Defence

3rd line

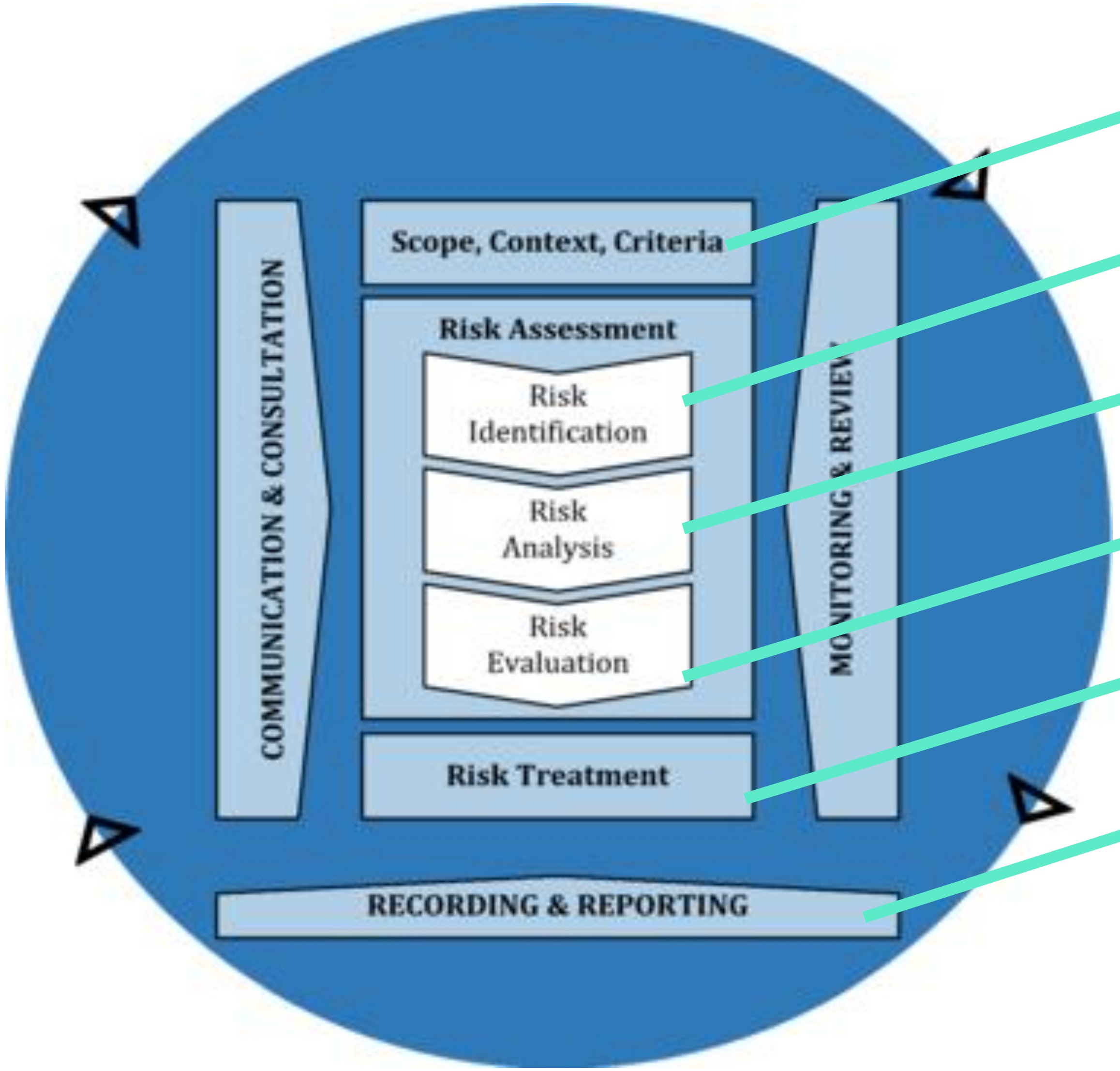
Internal Audit
Independent review of effectiveness of the risk

- **Audit & Risk Committee (ARC) and Commission**: Monitor the risk exposure of the organization; Setting up MCMC's Risk Committee

Risk Management Process

Systematic application of Policies, Procedures and Practices to the Risk Management Activities.

Risk Management Process (ISO31000:2018)



Description:

What is the **environment** in which your organization seeks to achieve its Objectives?

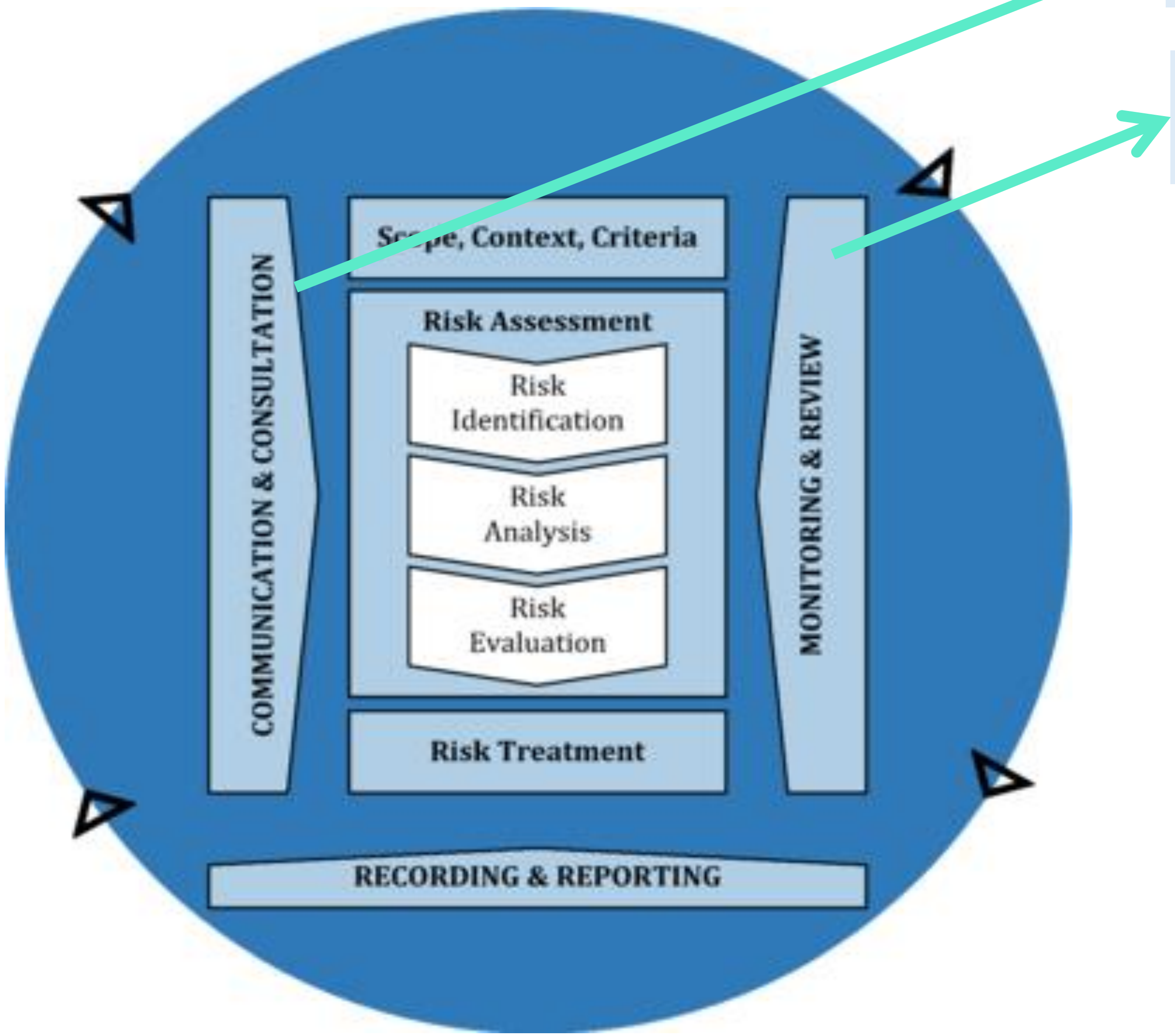
What **uncertainties** could prevent you from meeting the planned objectives ?

How serious would the risk be ?
In terms of **Likelihood and Impact.**

Is the risk **tolerable** ?

What actions can bring the risk to **acceptable levels** ?

What to report to the next level ?



Communicating and Interaction with **Stakeholders**

What is the **progress of risk treatment ?**
Any change to the risk ?

MCMC Strategic Objectives

Vision:

- Establishing a communications and multimedia industry that is **competitive**, **efficient** and increasingly **self-regulating**, **generating growth** to meet the economic and social needs of Malaysia.

MCMC Strategic Objectives

Missions:

We are committed to :

1. Promoting **access** to communications and multimedia services;
2. Ensuring **consumers enjoy choice** and a **satisfactory level of services** at **affordable prices**;
3. Providing **transparent regulatory processes** to facilitate **fair competition** and **efficiency** in the industry;
4. Ensuring **best use of spectrum and number resources**; and
5. Consulting regularly with consumers and service providers and facilitating **industry collaboration**.

MCMC Strategic Risks

- Regulatory Objectivity
- Policy Shift
- Rapidly Changing Trends
- Stakeholder Management & Communications
- Major Programmes
- Financial
- Fraud & Corruption
- Technological Changes
- Cyber Security

Risk Treatment

Process to **modify** the risk. The purpose of risk treatment is to select and implement options for addressing risk.

(ISO 31000:2018)

Mitigate

- **Reduce the likelihood**
- E.g., improving management controls and procedures.

- **Reduce the consequence**
- E.g., putting in place strategies to minimize adverse consequences

Accept

- **Current controls are deemed appropriate**
- Accept the Risk (absorb by prudent allowances or Policy)
- These must be monitored, and contingency plan developed

Transfer

- **Shift the responsibility for a risk to another party**
- E.g., Contract or Insurance

Avoid

- **Not to proceed with the activity or choosing an alternative approach** to achieve the same outcome
- Eliminate the cause of uncertainty that first introduced the risk

Risk Monitoring

Continual **checking**, **supervising**, critically **observing** or determining the status in order to **identify change from the performance level required** or expected.

(ISO 31000:2018)

Key Risk Indicators

- **Key Risk Indicators (KRI)** is the indicators of risk to business performance.
- It give **early warning** to identify a potential event that may cause the failure in achieving objectives.

When a KRI breaches its associated **threshold**, it should **trigger** a review, escalation, or management action.

Example:

% of suppliers with no business continuity management

Number of complaints received

% of exercise not exercised within last 12 months

% accident reported in a month

Key Risk Indicators vs Key Performance Indicators

KRIs are developed for the events with high inherent or residual risk.

Key Performance Indicator (KPI)

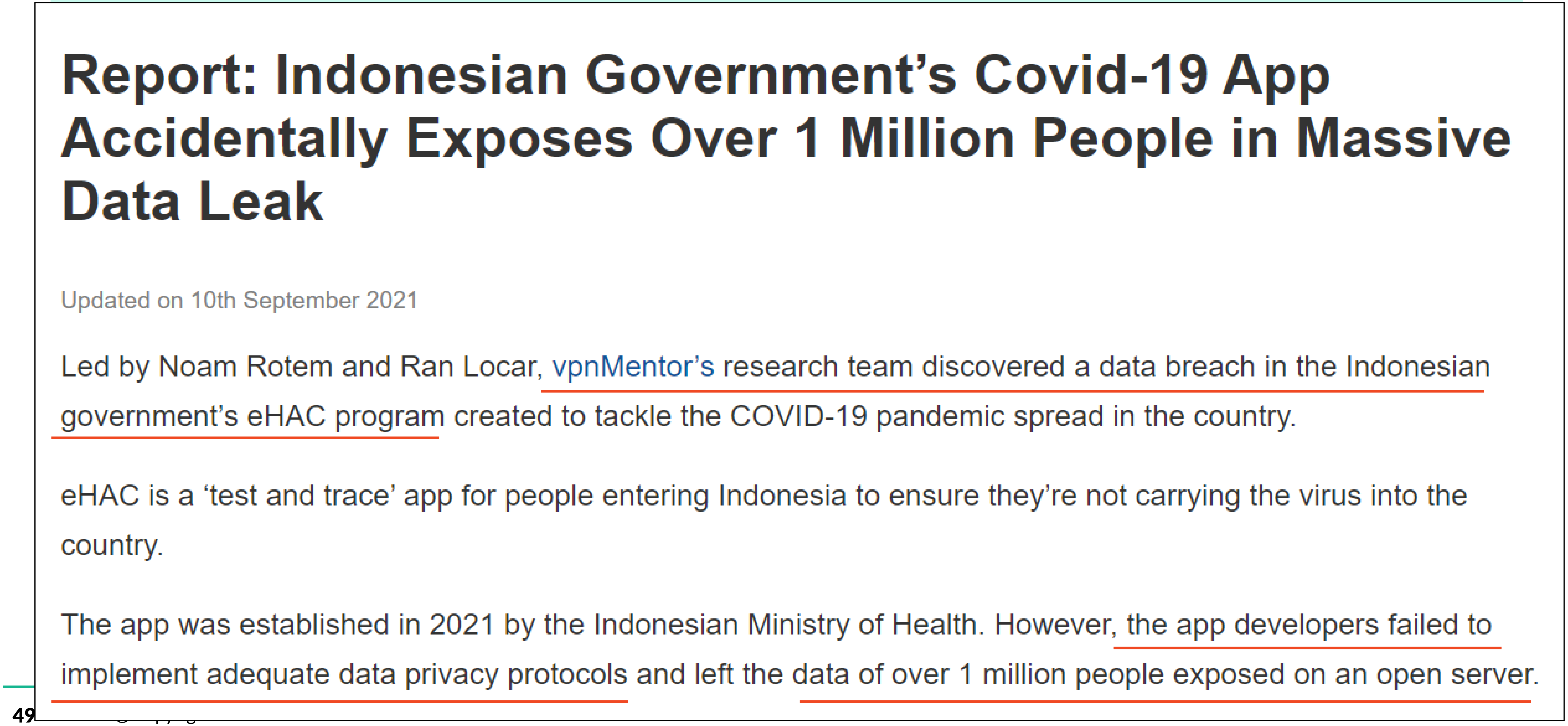
Key Risk Indicator (KRI)

*"A metric for indicating that the combined **likelihood** of an event and its **consequence** will exceed the organization's **risk appetite** and have a profoundly negative impact on an organization's ability to be successful".*

Key Performance Indicator (KPI), is a measure of **how well** something is being done.

Key Risk Indicator (KRI), is a measure to indicate **how risky** an activity is.

Case Study



Report: Indonesian Government's Covid-19 App Accidentally Exposes Over 1 Million People in Massive Data Leak

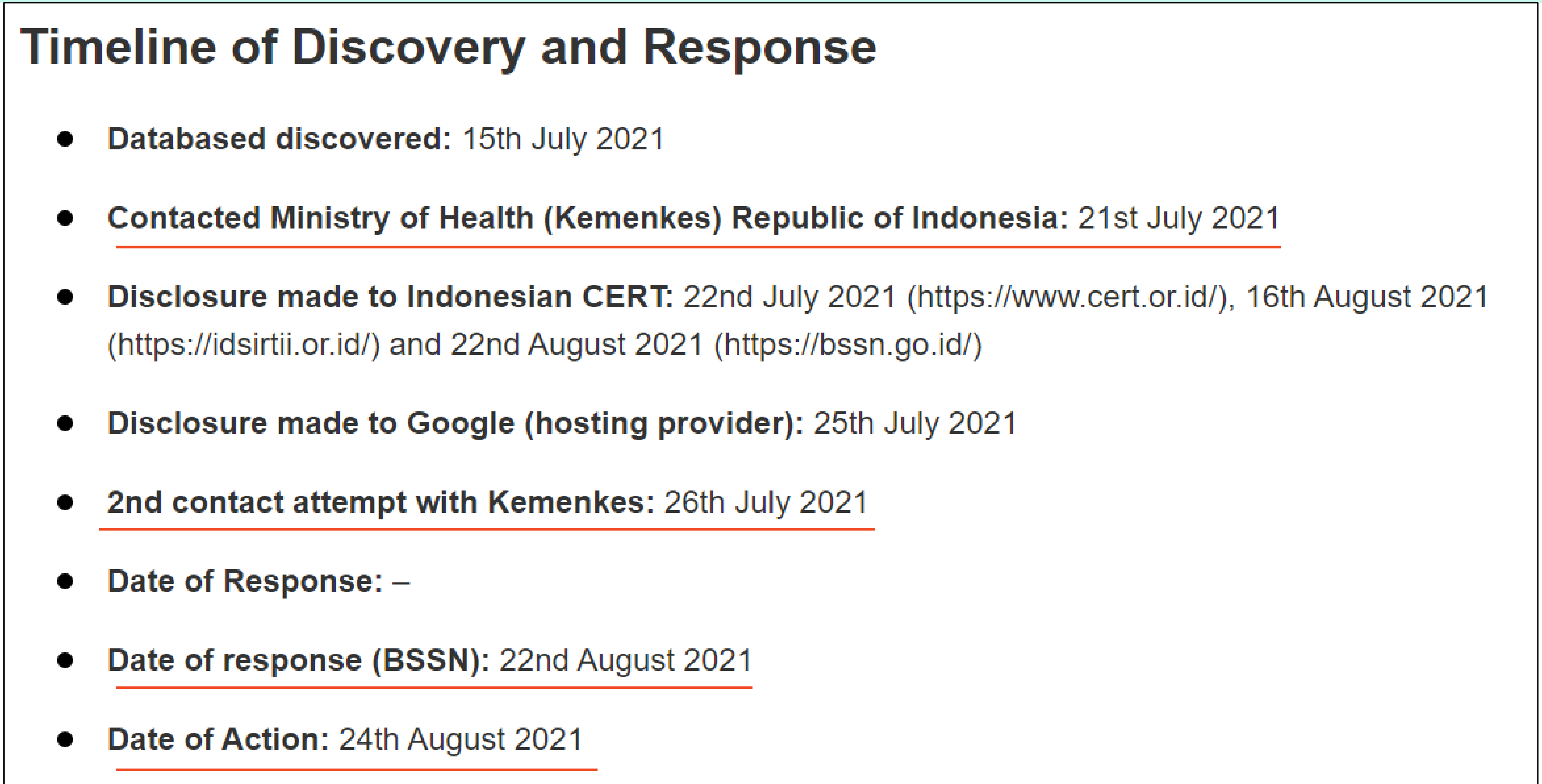
Updated on 10th September 2021

Led by Noam Rotem and Ran Locar, vpnMentor's research team discovered a data breach in the Indonesian government's eHAC program created to tackle the COVID-19 pandemic spread in the country.

eHAC is a 'test and trace' app for people entering Indonesia to ensure they're not carrying the virus into the country.

The app was established in 2021 by the Indonesian Ministry of Health. However, the app developers failed to implement adequate data privacy protocols and left the data of over 1 million people exposed on an open server.

Case Study



Timeline of Discovery and Response

- **Databased discovered:** 15th July 2021
- **Contacted Ministry of Health (Kemenkes) Republic of Indonesia:** 21st July 2021
- **Disclosure made to Indonesian CERT:** 22nd July 2021 (https://www.cert.or.id/), 16th August 2021 (https://idsirtii.or.id/) and 22nd August 2021 (https://bssn.go.id/)
- **Disclosure made to Google (hosting provider):** 25th July 2021
- **2nd contact attempt with Kemenkes:** 26th July 2021
- **Date of Response:** –
- **Date of response (BSSN):** 22nd August 2021
- **Date of Action:** 24th August 2021

Case Study

1. Any risk mitigation control should be in place to reduce the outsourcing risk? (before the incident occurred)

e.g., mitigation control could be any related policy / procedures / assessment / monitoring tools.

2. What could be done better to manage the crisis above? (after the incident occurred)

e.g., what are the possible response plan?

bit.ly/slido_mcmc2

Or head to **sli.do** and enter code **#886129**

4

What’s Next

Crisis Perpetually Appearing

LRT Trains Collide, Malaysia (2021)

COVID-19 Pandemic Flu Worldwide (2019 - Current)

Citizenship Data Leaked Indonesia (2021)

Myanmar Protest (2021)

Floods in Johor and Pahang, Malaysia (2021)

Personal Mobility Device Fire Singapore (2021)

So Many Scenarios to Plan...

What Can We Plan For ?

Plan for the consequences of losing these KEY RESOURCES

Equipment

Premises

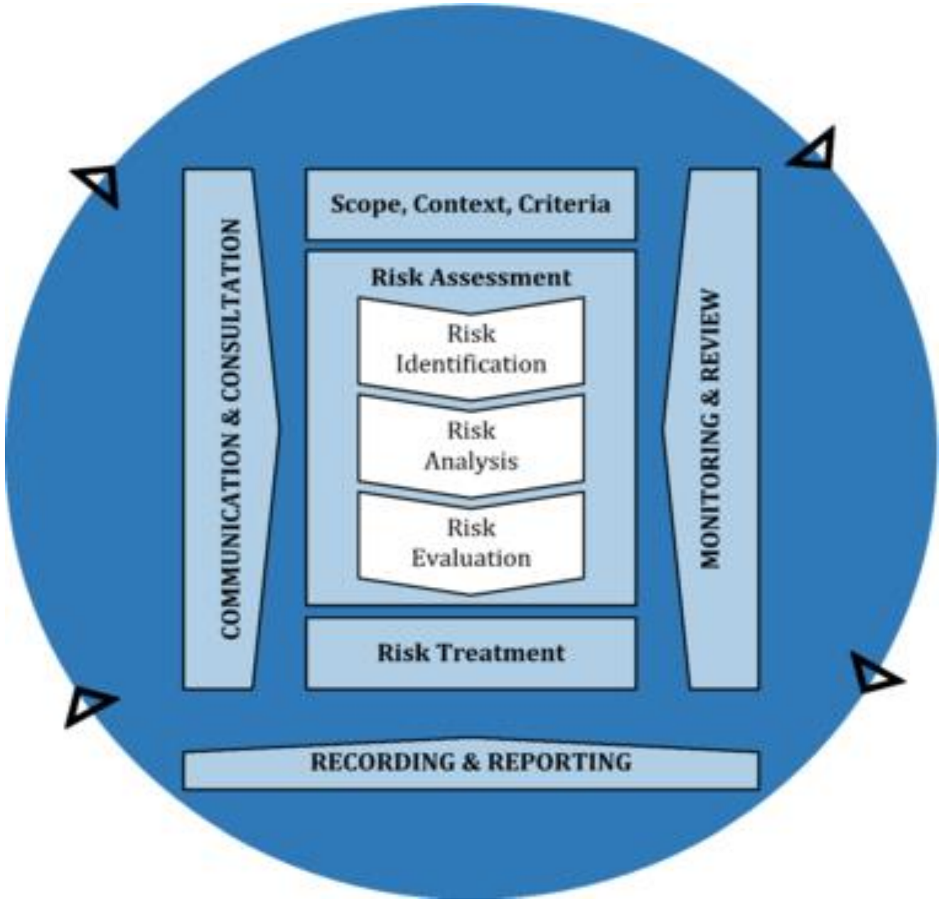
Supply Chain

Data

Staff

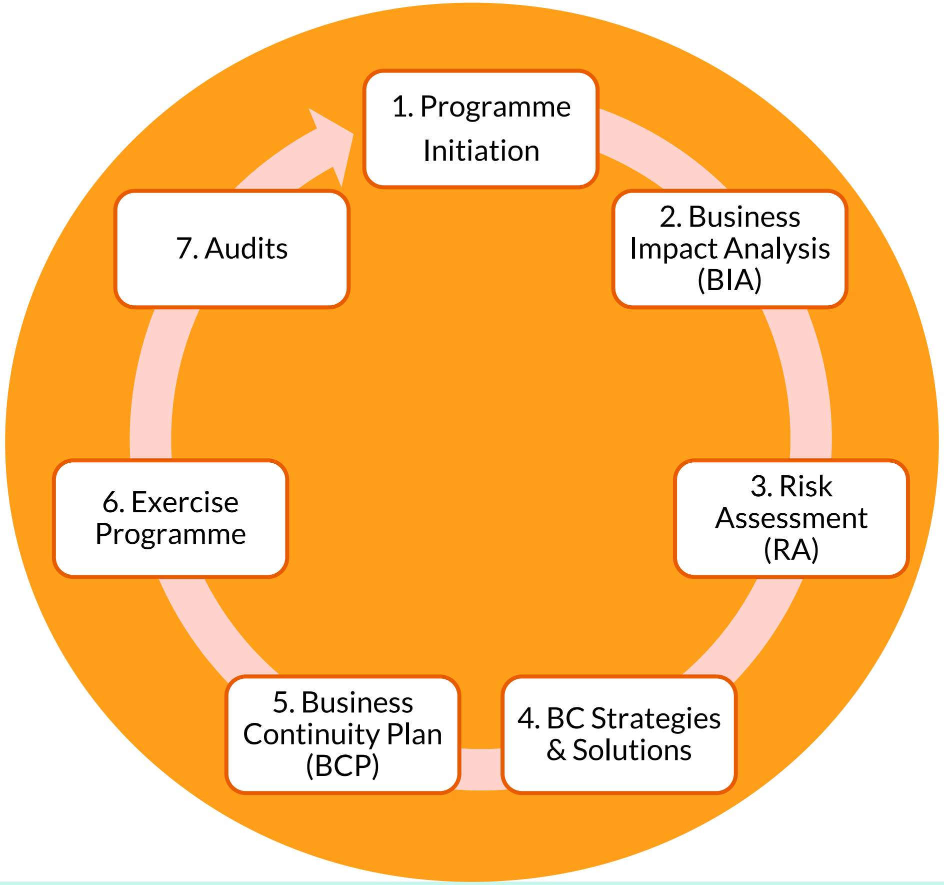
Enterprise Risk Management System (ERMS) & Business Continuity Management System (BCMS)

ERMS



Operational Risks could be mitigated by establishing BCMS

BCMS


1. Programme Initiation
2. Business Impact Analysis (BIA)
3. Risk Assessment (RA)
4. BC Strategies & Solutions
5. Business Continuity Plan (BCP)
6. Exercise Programme
7. Audits

It’s time to reassess your resilience

1. **Plan and prepare** for the next inevitable **disruption**

2. Establish a **crisis response team** and design a **crisis response plan** for top risks. Revisit the crisis management structure for effective response.

3. Build an **integrated resilience** program, coordinate the tactics, tools and technologies needed for an effective crisis response

4. Establish high-level resilience **governance**

5. **Monitor** ongoing **changes** and emerging **risks**

6. Foster a **culture** of resilience

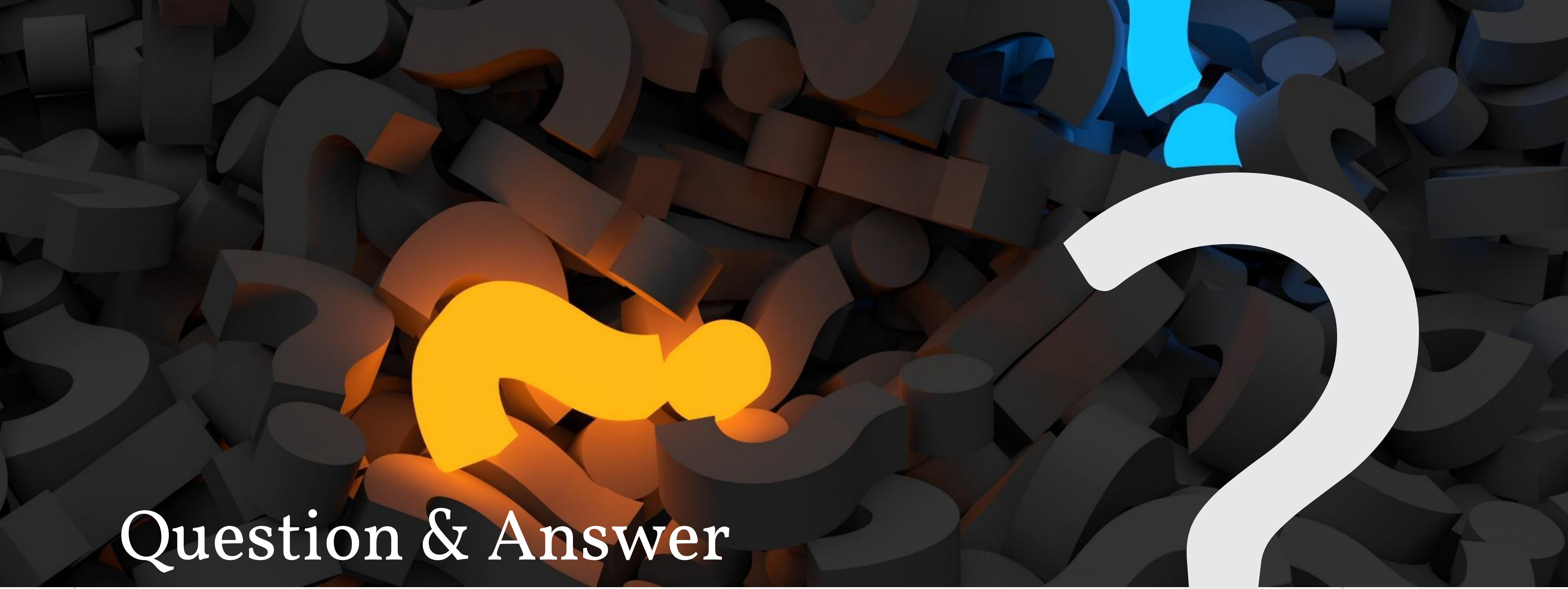
7. Establish **short-term mid-term and long-term planning** for enterprise risks.

Post-Training Questionnaire

To understand the effectiveness of the training, please spend **8 minutes** to answer the post-training questionnaire and submit it before you leave the training session.

bit.ly/post1022

Risk Management is Everyone’s Responsibility



Question & Answer

Evaluation Form

Tell us what you liked / disliked about our courses so that we can continuously improve to better suit your needs!

bit.ly/mcmc_erm2

BCP ASIA®
Preparing Business. Enhancing Minds

www.bcpasia.com.my

BCP ASIA SDN BHD

T. (60) 39212 4899

E. enquiry@bcpasia.com

BCP ASIA®

Preparing Business. Enhancing Minds

THANK YOU

www.bcpasia.com.my

Business Continuity • Enterprise Risk • Disaster Recovery • Crisis Management