

2022/23 Semester 1

---

## **IS3103 Information Systems Leadership and Communication**

### Lecture 9

# **IT Risk Management and Ethical Leadership**

A/Prof OH Lih Bin  
ohlb@comp.nus.edu.sg | 6516 3796 | COM2-0421

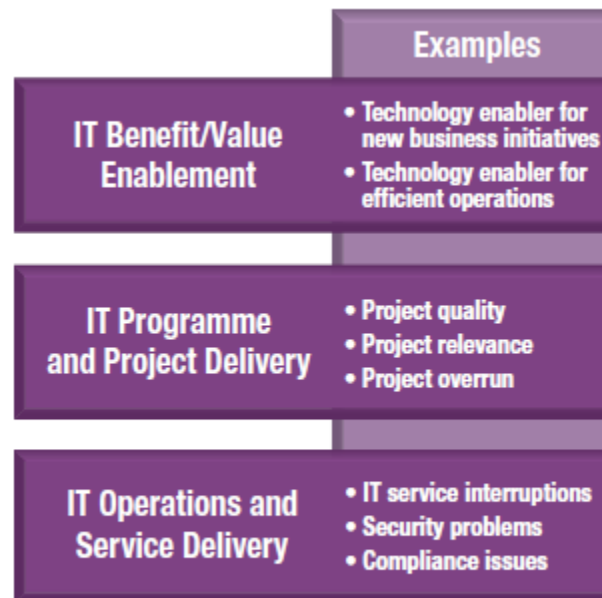
Department of Information Systems & Analytics  
NUS School of Computing



# IT-related Risk Management

► **IT Risk** is not limited to information security. It covers *all* IT-related risks, including:

- Late project delivery
- IT-business misalignment
- Not achieving enough value from IT
- Obsolete or inflexible IT architecture
- IT service delivery problems
- Legal and compliance issues



# COBIT (Control Objectives for Information Technologies)

## STRATEGY & GOVERNANCE

 EDM01  
IT Governance

 APO02  
IT Strategy

 MEA01  
Performance Measurement

 EDM02  
Business Value

 APO06  
Cost and Budget Management

 APO10  
Vendor Management

## FINANCIAL MANAGEMENT

 APO01  
IT Management and Policies

 APO04  
Innovation

 APO08 EDM05  
Stakeholder Relations

 BAI08  
Knowledge Management

 EDM04  
Cost Optimization

## IT Management & Governance Framework

A comprehensive and connected set of research to help you optimize and improve your core IT processes.

INFO~TECH  
RESEARCH GROUP

COBIT®  
AN ISACA® FRAMEWORK

## PEOPLE & RESOURCES

 APO07  
Human Resources Management

 ITRG01  
IT Organizational Design

 ITRG02  
Leadership, Culture and Values

 ITRG03  
Manage Service Catalogs

## SERVICE PLANNING & ARCHITECTURE

 APO03  
Enterprise Architecture

 APO09  
Service Management

 APO11  
Quality Management

## INFRASTRUCTURE & OPERATIONS


 BAI04  
Availability and Capacity Management

 BAI09  
Asset Management

 DSS01  
Operations Management

 BAI06  
Change Management

 BAI10  
Configuration Management

 DSS02  
Service Desk

## SECURITY & RISK

 DSS05  
Security Management

 EDM03 APO12  
Risk Management

 BAI07  
Release Management

 DSS03  
Incident and Problem Management

 APO13  
Security Strategy

 DSS06 MEA02  
Business Process Controls and Internal Audit

 MEA03  
External Compliance

 DSS04  
Business Continuity

 DSS04  
Disaster Recovery Planning

## APPS


 ITRG04  
Application Portfolio Management

 BAI03  
Enterprise Application Selection & Implementation

 BAI03  
Application Development Throughput

 BAI07  
Application Development Quality


 ITRG05  
Application Maintenance

 BAI05  
Organizational Change Management

## DATA & BI


 ITRG06  
Business Intelligence and Reporting

 ITRG07  
Data Architecture

 ITRG08  
Data Quality

 APO05  
Portfolio Management

 BAI01  
Project Management

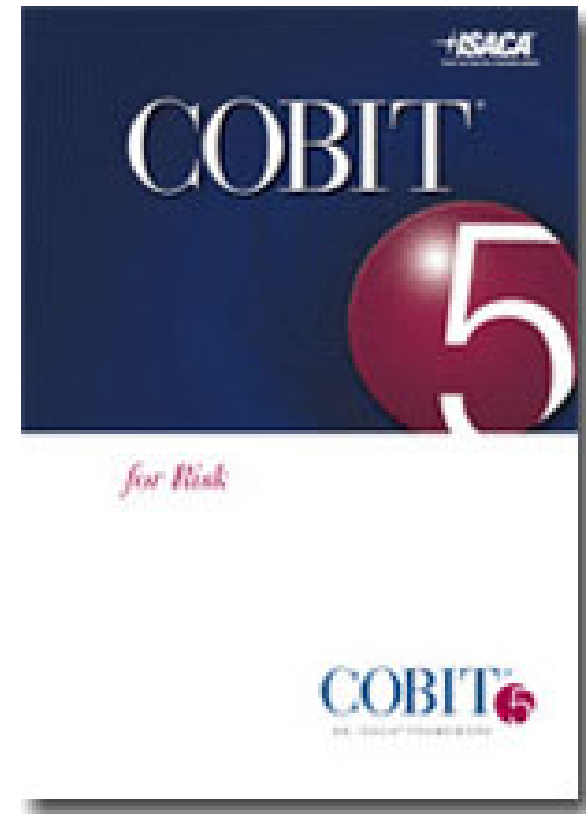
 BAI02  
Requirements Gathering

## PPM & PROJECTS

# Drivers for IT Risk Management

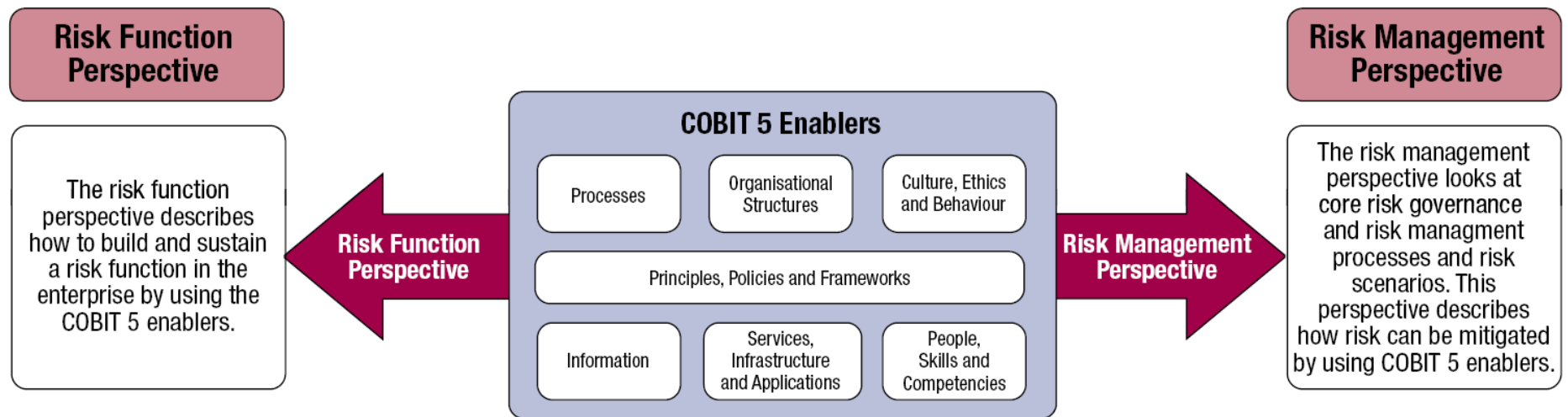
The *COBIT 5 for Risk* professional guide provides:

- Guidance on how to use the COBIT 5 framework to establish the *risk governance and management function(s)* for the enterprise
- Guidance and a structured approach on how to use the COBIT 5 principles to govern and manage IT risk



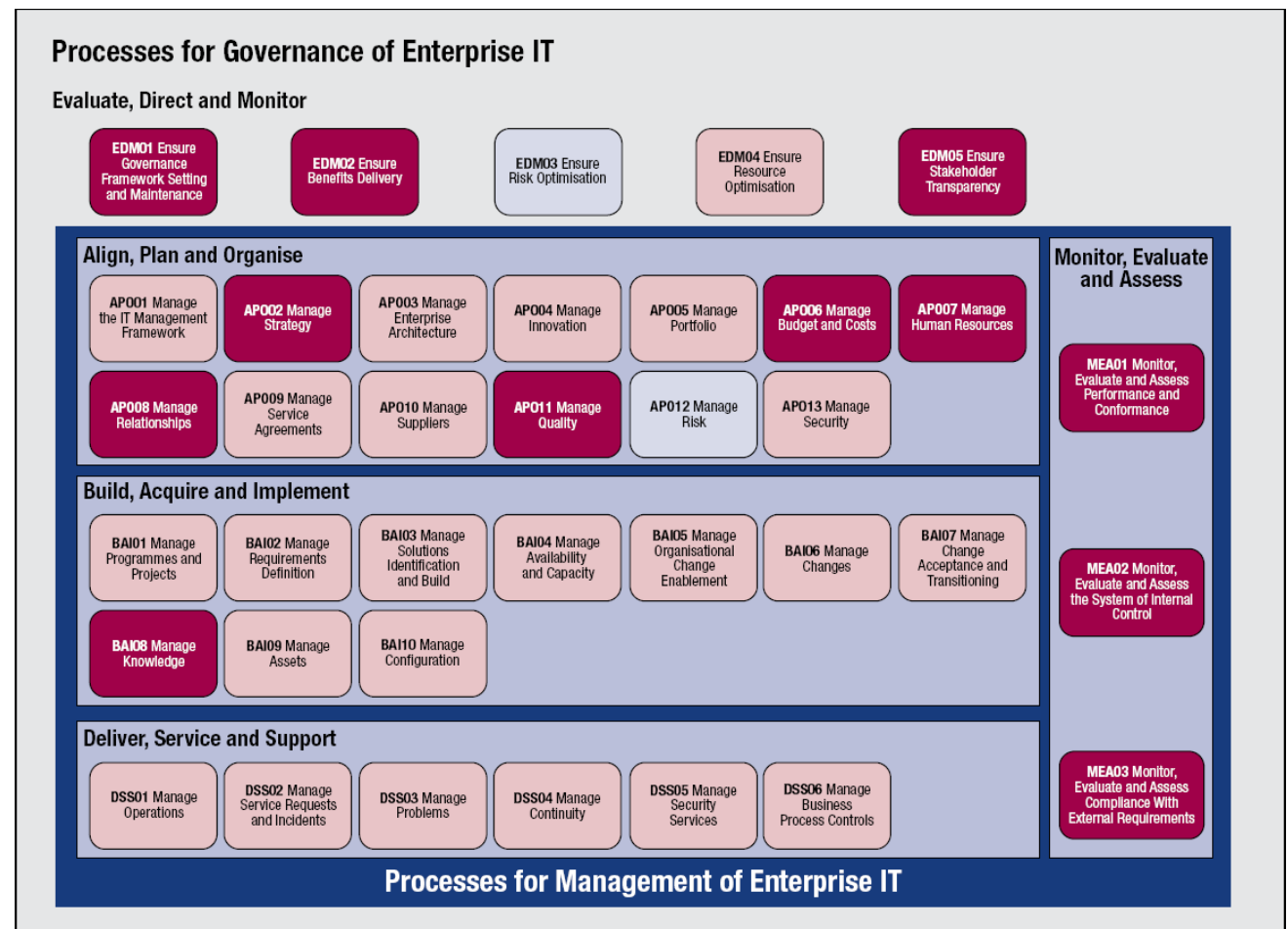
# Risk Perspectives

---



# Risk Function Perspective

- ▶ *COBIT 5 for Risk* identifies all COBIT 5 processes that are required to support the **risk function**:
  - Key supporting processes— **dark pink** (e.g., EDM01, EDM02, APO02, BAI08)
  - Other supporting processes – **light pink** (e.g., EDM04, APO01, BAI01)
- ▶ Core risk processes, shown in light blue are also highlighted—these processes support the **risk management** perspective:
  - EDM03 Ensure risk optimization
  - APO12 Manage risk



# Risk Management Perspective

---

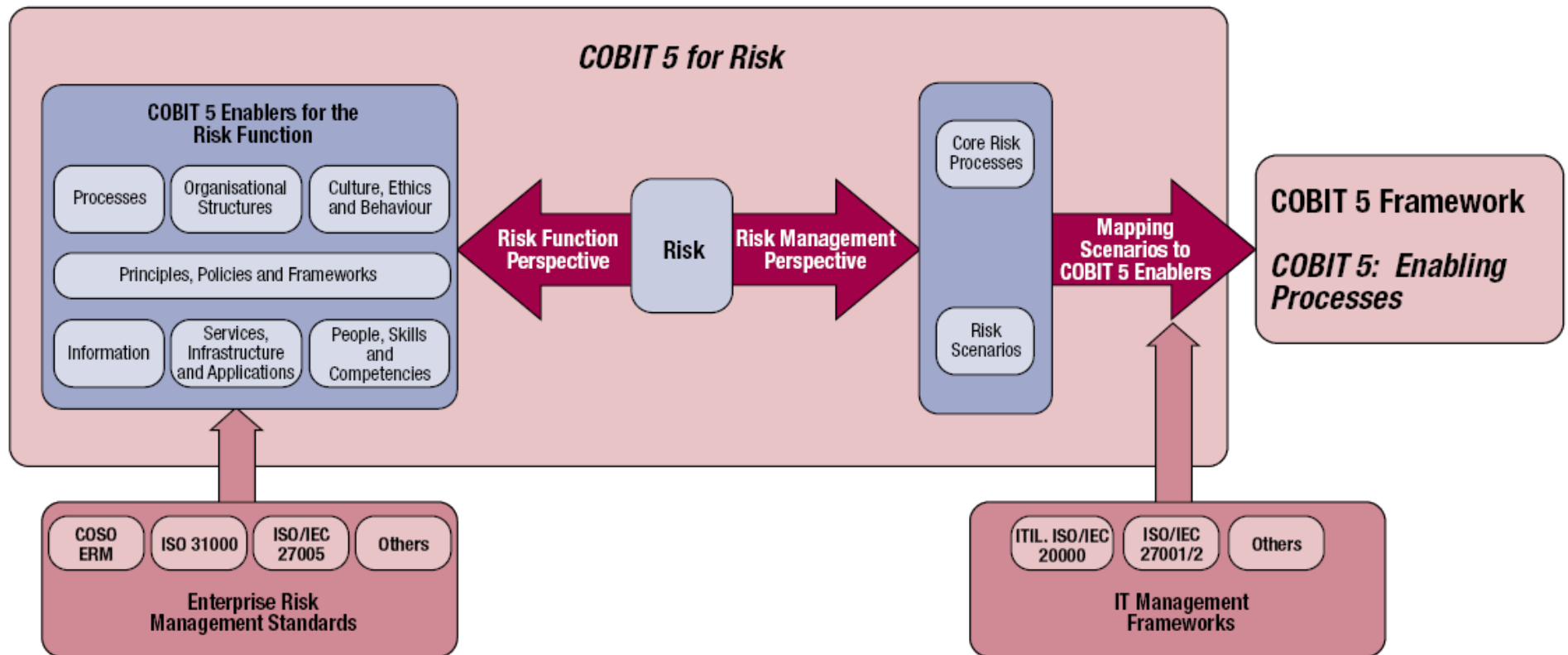
COBIT 5 Process Identification	Reasoning
<b>EDM03 Ensure Risk Optimisation</b>	<p>This process covers the understanding, articulation and communication of the enterprise risk appetite and tolerance and ensures identification and management of risk to the enterprise value that is related to IT use and its impact. The goals of this process are to:</p> <ul style="list-style-type: none"><li>• Define and communicate risk thresholds and make sure that key IT-related risk is known.</li><li>• Effectively and efficiently manage critical IT-related enterprise risk.</li><li>• Ensure IT-related enterprise risk does not exceed risk appetite.</li></ul>
<b>AP012 Manage Risk</b>	<p>This process covers the continuous identification, assessment and reduction of IT-related risk within levels of tolerance set by enterprise executive management. Management of IT-related enterprise risk should be integrated with overall ERM. The costs and benefits of managing IT-related enterprise risk should be balanced by:</p> <ul style="list-style-type: none"><li>• Collecting appropriate data and analysing risk</li><li>• Maintaining the risk profile of the enterprise and articulating risk</li><li>• Defining the risk management action portfolio and responding to risk</li></ul>

*COBIT 5 for Risk* provides specific guidance related to all enablers for the effective management of risk:

- The core **Risk Management processes** used to implement effective and efficient risk management for the enterprise to support stakeholder value
- **Risk Scenarios**, i.e., the key information item needed to identify, analyze and respond to risk; risk scenarios are the concrete, tangible and assessable representation of risk
- How **COBIT 5 enablers** can be used to **respond** to unacceptable risk scenarios



# How *COBIT 5 for Risk* relates to and aligns with other standards





# Alignment with other standards

---

- ▶ *COBIT 5 for Risk*—much like COBIT 5 itself—**is an umbrella approach** for the provisioning of risk management activities.
- ▶ *COBIT 5 for Risk* is **positioned in context** with the following risk-related standards:
  - ▶ COSO Enterprise Risk Management
  - ▶ ISO 31000:2009 – Risk Management
  - ▶ ISO 27005:2011 – Information Security Risk Management
  - ▶ ISO 27001:2013 – Information Security Management



# Other RM standards

---

- ▶ **COSO Enterprise Risk Management**

- ▶ *COBIT 5 for Risk* **addresses all** of the components defined in COSO ERM.
- ▶ Although *COBIT 5 for Risk* focuses less on control, it provides **linkages to enablers**—management practices in the COBIT 5 framework.
- ▶ The **essentials with regards to both control and general risk management** as defined in COSO ERM are present in *COBIT 5 for Risk*, either through the:
  - ▶ Principles themselves and the framework's conceptual design
  - ▶ Process model and additional guidance provided in the framework



# Other RM standards

---

## ▶ **ISO 31000:2009 – Risk Management**

- ▶ *COBIT 5 for Risk* **addresses all** ISO 31000 principles, through the *COBIT 5 for Risk* principles and enablers themselves
- ▶ In addition, the framework and process model aspects are covered in greater detail by the *COBIT 5 for Risk* process model.
- ▶ All elements are included in *COBIT 5 for Risk* and are often expanded on or elaborated in greater detail, specifically for IT risk management.



# Other RM standards

---

- ▶ **ISO 27005:2011 – Information security risk management**

- ▶ *COBIT 5 for Risk* **addresses all** of the components described within ISO 27005. Some of the elements are structured or named differently.
- ▶ *COBIT 5 for Risk* **takes a broader view** on IT risk management compared with ISO 27005 which is focused on the management of security-related risk.
- ▶ There is a **stronger emphasis** in *COBIT 5 for Risk* on processes and practices to ensure the *alignment with business objectives*, the acceptance throughout the organization and the completeness of the scope, amongst other factors.

# Risk Management in COBIT 5

- In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process. **These include risk-related roles.** (RACI: responsible, accountable, consulted or informed)

Align, Plan and Organise

AP012 RACI Chart																											
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer	
AP012.01 Collect data.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R	
AP012.02 Analyse risk.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C	
AP012.03 Maintain a risk profile.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C	
AP012.04 Articulate risk.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C	
AP012.05 Define a risk management action portfolio.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C	
AP012.06 Respond to risk.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R	

Align, Plan and Organise

# Using Risk Scenarios for Governance of Enterprise IT

- ▶ *COBIT 5 for Risk* provides a comprehensive set of generic risk scenarios. These should be used as a reference to reduce the chance of overlooking major/common risk scenarios.
- ▶ *COBIT 5 for Risk* provides:
  - ▶ 111 risk scenario examples
  - ▶ Across 20 scenario categories

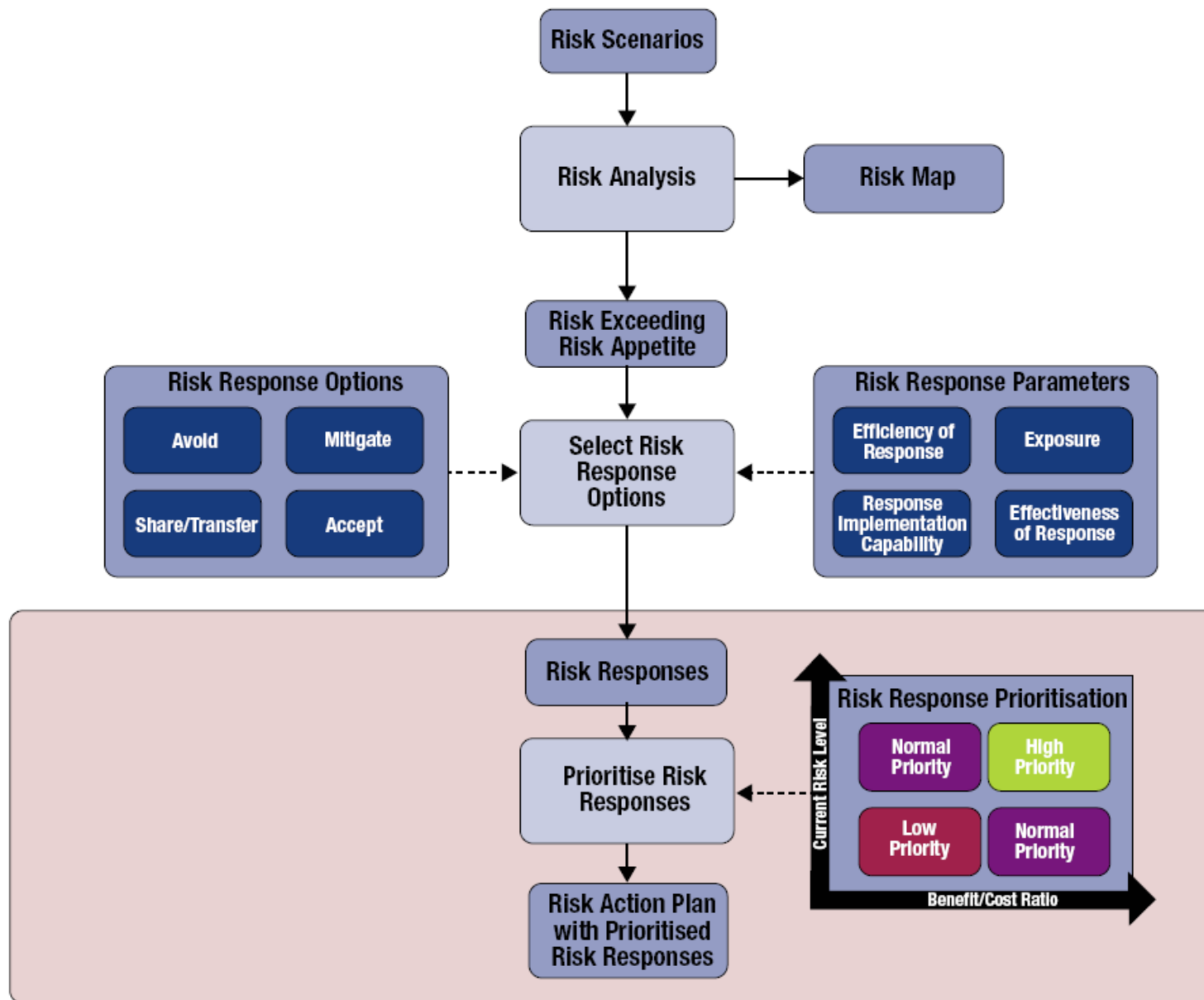
**Figure 38—Example Risk Scenarios (cont.)**

Ref.	Risk Scenario Category	Risk Type			Example Scenarios	
		IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Positive Example Scenarios
0801	Infrastructure (hardware, operating system and controlling technology) (selection/ implementation, operations and decommissioning)	P	S	P	New (innovative) infrastructure is installed and as a result systems become unstable leading to operational incidents, e.g., Bring your own device (BYOD) programme.	Appropriate testing is conducted before setting infrastructure into the production environment to ensure the availability and proper functioning of the entire system.
0802		P	S	P	The systems cannot handle transaction volumes when user volumes increase.	
0803		P	S	P	The systems cannot handle system load when new applications or initiatives are deployed.	
0804		P	S	P	Intermittently, there are failures of utilities (telecom, electricity).	Second line utilities are foreseen and stand by 24/7 to support the continuous execution of business critical transactions.
0805		P	S	P	The IT in use is obsolete and cannot satisfy new business requirements (networking, security, database, storage, etc.).	IT is an innovator, ensuring a two-way interaction between business and IT.
0806				P	Hardware fails due to overheating.	

# Risk Mitigation

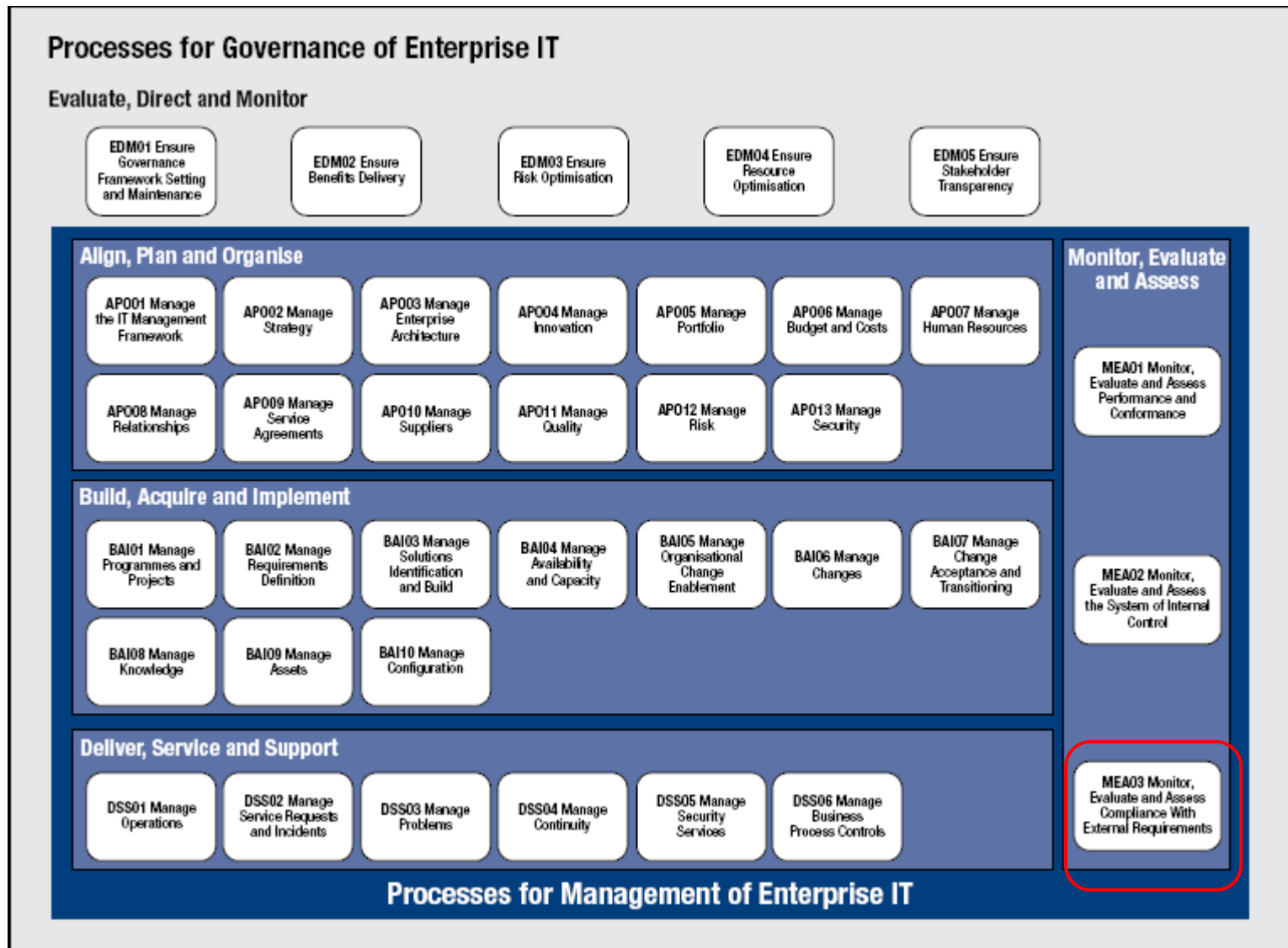
- ▶ For each of the 20 risk scenario categories, potential mitigating actions relating to all seven COBIT 5 enablers are provided, with a reference, title and description for each enabler that can help to mitigate the risk.

D.3. Scenario 3: IT Investment Decision Making		
Risk Scenario Category		IT investment decision making
Principles, Policies and Frameworks Enabler		
Reference		Contribution to Response to Scenario
Programme/Project management policy		The policy should define who needs to be involved in investment decisions and the chain of approval.
Process Enabler		
Reference	Title	Management Practice
AP005.06	Manage benefits achievement.	Monitor the benefits of providing and maintaining appropriate IT services and capabilities, based on the agreed-on and current business case.
AP006.02	Prioritise resource allocation.	Implement a decision-making process to prioritise the allocation of resources and rules for discretionary investments by individual business units. Include the potential use of external service providers and consider the buy, develop and rent options.
AP006.03	Create and maintain budgets.	Prepare a budget reflecting the investment priorities supporting strategic objectives based on the portfolio of IT-enabled programmes and IT services.
AP007.01	Maintain adequate and appropriate staffing.	Evaluate staffing requirements on a regular basis or on major changes to the enterprise or operational or IT environments to ensure that the enterprise has sufficient human resources to support enterprise goals and objectives. Staffing includes both internal and external resources.
BAI01.03	Manage stakeholder engagement.	Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information that reaches all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.
BAI03.04	Procure solution components.	Procure solution components based on the acquisition plan in accordance with requirements and detailed designs, architecture principles and standards, and the enterprise's overall procurement and contract procedures, QA requirements, and approval standards. Ensure that all legal and contractual requirements are identified and addressed by the supplier.





# Compliance in COBIT 5



# Compliance in COBIT 5



- The MANAGEMENT Monitor, Evaluate and Assess domain contains a compliance focused process: **MEA03 Monitor, evaluate and assess compliance with external requirements.**
- **Process Purpose Statement**
  - Ensure that the enterprise is compliant with all applicable external requirements.
- **Process Description**
  - Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements.
  - Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.

# Compliance in COBIT 5

- In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process. **These include a compliance-related role.**  
(RACI: responsible, accountable, consulted or informed)

MEA03 RACI Chart																				
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development
MEA03.01 Identify external compliance requirements.					A	R										R	R	R		
MEA03.02 Optimise response to external requirements.		R	R	R	A	R	I		R							R	R	R	I	R
MEA03.03 Confirm external compliance.	I	R	R	R	R	R	I	I	C							A	I	R	C	C
MEA03.04 Obtain assurance of external compliance.	I	I	I	I	C	C	I		C							C	A	R	C	C

Source: COBIT® 5: Enabling Processes, page 213. © 2012 ISACA® All rights reserved.

# Compliance with ICT-Related Laws

---

- ▶ Computer Misuse and Cybersecurity Act (CMCA)
- ▶ Personal Data Protection Act (PDPA)
- ▶ Spam Control Act
- ▶ Protection from Online Falsehoods and Manipulation Act (POFMA)
  
- ▶ Copyright/Patent Laws
- ▶ Undesirable Publications Act



THE STATUTES OF THE REPUBLIC OF SINGAPORE

COMPUTER MISUSE AND CYBERSECURITY ACT

(CHAPTER 50A)

(Original Enactment: Act 19 of 1993)

REVISED EDITION 2007

(31st July 2007)

*Prepared and Published by*  
THE LAW REVISION COMMISSION  
UNDER THE AUTHORITY OF  
THE REVISED EDITION OF THE LAWS ACT (CHAPTER 275)

Informal Consolidation – version in force from 1/6/2017



REPUBLIC OF SINGAPORE  
GOVERNMENT GAZETTE  
ACTS SUPPLEMENT

*Published by Authority*

NO. 25] FRIDAY, DECEMBER 7 [2012

The following Act was passed by Parliament on 15th October 2012 and assented to by the President on 20th November 2012:—

PERSONAL DATA PROTECTION ACT 2012

(No. 26 of 2012)

I assent.

TONY TAN KENG YAM,  
*President.*  
20th November 2012.

**Date of Commencement:** 2nd January 2013 Parts I, II, VIII, sections 39, 40, 42, 49 to 66, 67(2) and (3), 68, the First, Seventh and Ninth Schedules

**Date of Commencement:** 2nd December 2013 Sections 36, 37, 38 and 41

**Date of Commencement:** 2nd January 2014 Sections 43 to 48, 67(1) and the Eighth Schedule

**Date of Commencement:** 2nd July 2014 Parts III to VII, the Second, Third, Fourth, Fifth and Sixth Schedules

An Act to govern the collection, use and disclosure of personal data by organisations, and to establish the Do Not Call Register and to provide for its administration, and for matters connected therewith, and to make related and consequential amendments to various other Acts.

*[Act 22 of 2016 wef 01/10/2016]*



THE STATUTES OF THE REPUBLIC OF SINGAPORE

SPAM CONTROL ACT

(CHAPTER 311A)

(Original Enactment: Act 21 of 2007)

REVISED EDITION 2008  
(31st July 2008)

*Prepared and Published by*  
THE LAW REVISION COMMISSION  
UNDER THE AUTHORITY OF  
THE REVISED EDITION OF THE LAWS ACT (CHAPTER 275)

Informal Consolidation – version in force from 1/10/2016

Protection from Online Falsehoods  
and Manipulation Bill

Bill No. 10/2019.

*Read the first time on 1 April 2019.*

PROTECTION FROM ONLINE FALSEHOODS  
AND MANIPULATION ACT 2019

(No. of 2019)

ARRANGEMENT OF SECTIONS

PART 1  
PRELIMINARY

Section

1. Short title and commencement
2. General interpretation
3. Meaning of “communicate”
4. Meaning of “in the public interest”
5. Purpose of Act
6. Appointment of Competent Authority

PART 2

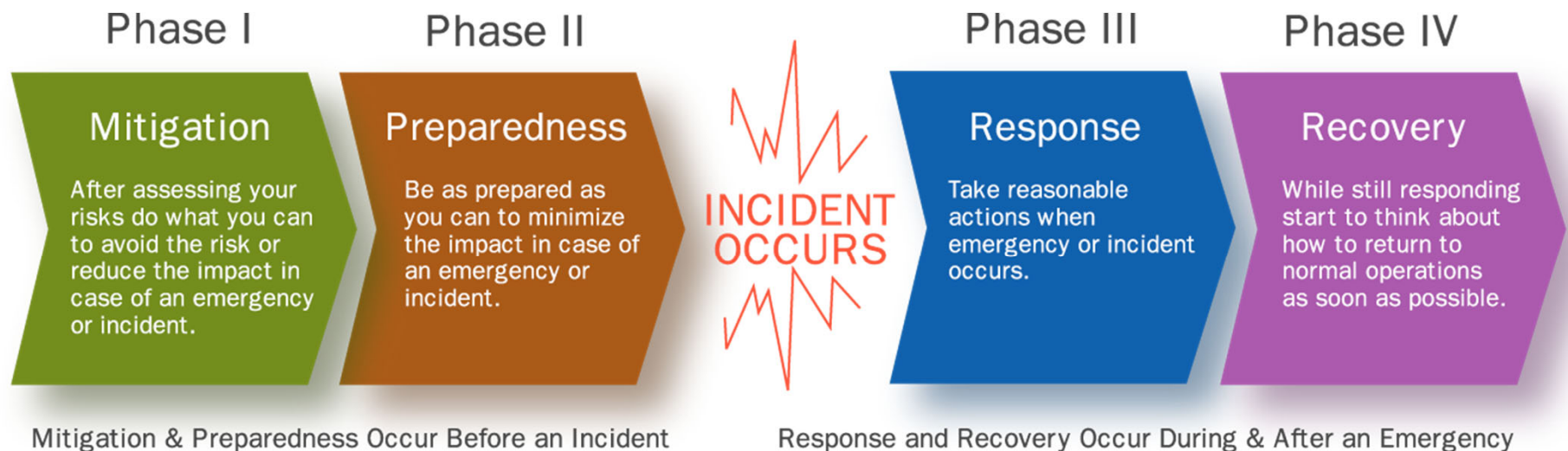
PROHIBITION OF COMMUNICATION OF  
FALSE STATEMENTS OF FACT IN SINGAPORE

7. Communication of false statements of fact in Singapore
8. Making or altering bots for communication of false statements of fact in Singapore
9. Providing services for communication of false statements of fact in Singapore

# Business Continuity Planning

---

The business continuity plan (BCP) details what you'll need to do to keep your business running or get it back up and running in a disaster.



Phases of business continuity planning



# Business Continuity Management (BCM)

---

- ▶ Business continuity is an organization's ability to ensure operations and core business functions are not severely impacted by a disaster or unplanned incident that take critical systems offline
- ▶ BCM exists to avoid any interruptions that could lead to either significant losses or a failure to achieve the organization's principal objectives



# The Role of Business Continuity Manager

---



## Objective

Ensure that business continuity is in place and the organization has a proven ability to recover.



## Tasks

Set policy  
Create BCM process  
Provide business continuity tools  
Implement BCM process  
Ensure staff is aware of duties  
Assess the maturity and quality of BCM and report issues and risks  
Ensure the business continuity solutions and plans are tested



## Deliverables

Policy  
BCM process  
Training  
Exercises  
Tests  
Management reports





# Business Continuity Management Software

- ▶ Business continuity software is an application or suite designed to make BCM processes, metrics and compliance more efficient and accurate.
- ▶ Examples of BCM program solutions
  - ▶ RPx Recovery Planner
  - ▶ Fusion Framework System
  - ▶ MetricStream
  - ▶ Oracle Risk Management Cloud
  - ▶ ClearView
  - ▶ MaestroRS
  - ▶ ParaSolution
  - ▶ Quantivate Business Continuity software

- ▶ <https://www.gartner.com/reviews/market/business-continuity-management-program-solutions>



The screenshot shows the 'Fusion Framework System - Risk Management Application' interface. It includes a 'Welcome' message, a 'Risk Manager' section with a 'Risk Count' of 7, and a 'Top 5 Risk' table. Below these are sections for 'My Risks' and 'My Controls'.

Risk Name	Impact	Likelihood	Top 5 Risk
Trade Order Entry Error	Catastrophic	Not likely to occur even...	Within a day
Infrastructure Failure	Significant	Somewhat likely to occ...	Within a day
Financial Reporting Error	Significant	Not likely to occur even...	Within a day
Internal Theft of Cash...	Significant	Not likely to occur even...	Within a day
Manufacturing Disrupti...	Material	Not likely to occur even...	Within a day

Control Name	Description
Automated Enhanced Due Diligence Check	Before monetary transactions are wired or sent...
Automated Equity Reconciliation Block	Upon trade entrance, the trading system will au...
Automated System Reconciliation	Automated journal entry systems identify and L...
Backup Manufacturing Plants	In the event of a manufacturing facility failing, t...
Code of Conduct Attestation	Upon hiring and on an annual basis, all assoc...

*Never waste the opportunities offered by a good crisis.*

*—Niccolò Machiavelli*

# Leadership in Crisis

---

- ▶ A *crisis* is any major unpredictable event that has the potential to damage an organization and, in extreme cases, to threaten its survival.
- ▶ Crisis Types
  - ▶ Public perception: negative stories about the organization's products, personnel, or services; negative rumors; blogs and websites
  - ▶ Natural disasters: tornadoes, hurricanes, mudslides, wildfires, blizzards, earthquakes, volcano eruptions
  - ▶ Product or service: product recalls, food-borne illnesses, concern about products and services generated by the media
  - ▶ Terrorist attacks: bombings, hijackings, abductions, poisonings
  - ▶ Economic: cash shortages, bankruptcies, hostile takeovers, accounting scandals
  - ▶ Human resource: workplace violence, strikes, labor unrest, discrimination, sexual harassment, school and workplace shootings, theft, fraud
  - ▶ Industrial: mine collapses, nuclear accidents, fires, explosions
  - ▶ Oil and chemical spills: tanker and railway spills, pipeline and well leaks
  - ▶ Transportation: train derailments, plane crashes, truck accidents, multi- vehicle pileups
  - ▶ Outside environment: collapse of financial systems, rising fuel prices, deregulation, nationalization of private companies, mortgage crisis



# Crisis Stages

---

## ▶ Stage 1: Pre-crisis

- ▶ Organizations spend most of their time between crises. During these periods of normalcy, leaders typically assume that the risks of a crisis occurring are low.
- ▶ As a leader, you'll need to fight the tendency to become complacent.

## ▶ Stage 2: Crisis Event

- ▶ This stage begins with a "trigger event" that initiates the crisis and ends when the crisis is resolved.
- ▶ During the crisis event, the focus shifts to damage control.
- ▶ The group implements its crisis management plans, communicates to internal and external publics, responds to outside pressures, and tries to resume normal operations.
- ▶ Work closely with business continuity manager
- ▶ Containing the problem is an important component of this stage.

## ▶ Stage 3: Post-crisis

- ▶ The post-crisis stage begins when the immediate danger is past and the organization has been able to resume its normal operations.
- ▶ This is a period of evaluation, analysis, and restoration. Crisis-savvy leaders try to learn from their experiences



# Crisis Leadership

---

- ▶ Pre-crisis Leadership
  - ▶ Recognize Danger Signs
  - ▶ Look for Trouble
  - ▶ Create a Crisis Management Plan (CMP)
- ▶ Leading during the Crisis Event
  - ▶ Initiate Action and Coordinate Activities
  - ▶ Act as a Spokesperson
  - ▶ Connect with Vision and Values
- ▶ Post-crisis Leadership
  - ▶ Rebuild the Organization's Image
  - ▶ Learn from the Experience
  - ▶ Promote healing

---

*A degree of paranoia helps protect organizations.*

—Yiannis Gabriel

Here is a non-exhaustive list of some of the notable data breaches in Singapore:

Company & Source	Number of Consumers Affected	Type of Data Leaked	Fine Amount	Date of Data Leak
Integrated Health Information Systems (IHIS) & SingHealth <sup>1</sup>	1.5 million patients	Names, IC numbers, addresses, gender, race & dates of birth	S\$1 million (IHIS S\$750,000 + SingHealth S\$250,000)	Jun - Jul 2018
Grab <sup>2</sup>	21,541 drivers & passengers	Profile pictures, names & vehicle plate numbers	S\$10,000	Aug 2019
ST Logistics <sup>3</sup>	2,400 Mindef & SAF personnel	Full names and NRIC numbers & a combination of contact numbers, email addresses or residential addresses	S\$8,000	Dec 2019
HMI Institute of Health Sciences <sup>3</sup>	110,080 customers (SAF servicemen, HMI staff etc.)	Full names, NRIC numbers, dates of birth, home addresses & email addresses	S\$35,000	
RedDoorz <sup>4</sup>	5.9 million customer records	Names, contact numbers, email address, date of birth, hashed passwords & their booking information	S\$74,000	Sep 2020
GeniusU <sup>5</sup>	1.2 million users' personal data	First and last names, e-mail addresses, location information and last sign-in IP addresses	S\$35,000	Jan 2021
MyRepublic <sup>6</sup>	79,388 users	Scanned copies of both sides of NRICs, workpasses & proof of residential addresses	S\$60,000	Aug 2021

Sources:

<sup>1</sup><https://www.straitstimes.com/singapore/singapores-privacy-watchdog-fines-ihis-750000-singhealth-250000-for-data-breach>

<sup>2</sup><https://www.straitstimes.com/tech/grab-fined-10000-for-fourth-data-privacy-breach-in-two-years>

<sup>3</sup><https://www.todayonline.com/singapore/2-firms-fined-s43000-total-over-personal-data-breaches-affecting-mindef-saf-personnel>

<sup>4</sup><https://www.businesstimes.com.sg/garage/data-breach-at-reddoorz-hit-6m-customers-hospitality-platform-fined-s74000>

<sup>5</sup><https://tnp.straitstimes.com/lifestyle/tech/edu-tech-firm-geniusu-fined-35000-data-leak-affecting-126m-users>

<sup>6</sup><https://www.channelnewsasia.com/singapore/myrepublic-data-breach-nric-personal-information-2168531>

# Why are unethical decisions being made?

---

<b>Moral Disengagement</b>	<b>Examples</b>
<b>Moral Justification</b>	If I do not present the data in such a way, many jobs would be cut and many of our staff would be made redundant.
<b>Advantageous Comparison</b>	It is ok to use unlicensed copies of XX software as the high performers are doing it.
<b>Displacement of Responsibility</b>	I had no choice as I am just doing what my boss told me to do, even though I know it is not right.
<b>Euphemistic Labelling</b>	I am not hacking, I am just doing research on the capabilities of the program that I developed.

- Adapted from Albert Bandura, 1979



# Ethical Challenges of Leadership

---

## ▶ Challenge of Power

- ▶ Leader must decide when to employ power, what types of power to use, and how much power s/he wishes to exert over followers
- ▶ Is it ethical to dominate followers and demand action, or should power be distributed?
- ▶ Is it ethical for a leader to demand compliance when a follower has a moral objection to the leader's request?

## ▶ Challenge of Privilege

- ▶ Leaders deserve additional privileges because they have a broader range of responsibilities than followers, but just how far should these benefits extend?
- ▶ Is it ethical for a leader to take advantage of his or her position to achieve personal power or prestige?
- ▶ Should a leader's concern always be for the good of the collective?



# Ethical Challenges of Leadership

---

## ▶ Challenge of Consistency

- ▶ Leaders deal with a variety of followers, relationships, and situations, making it difficult to behave consistently
- ▶ Situational and relational approaches to leadership demand “inconsistent” leadership behavior based on factors such as followers’ readiness, tasks, in-group/out-group membership
- ▶ Deciding when to bend the rules and for whom is also problematic
- ▶ Some degree of inconsistency appears inevitable, but leaders should avoid acting arbitrarily and unfairly
- ▶ They should try to be equitable with followers, making exceptions only after careful thought

*Wrong is wrong, no matter who does it or says it.*

*—Malcolm X*





# Ethical Challenges of Leadership

---

## ▶ Challenge of Information Management

- ▶ Leaders typically have access to more information than do followers
- ▶ Leaders practice deception for personal or group interest - whether to tell the truth? ("distort reality")
- ▶ When to release information and to whom?
- ▶ Deny having knowledge in their possession
- ▶ Put followers in moral binds by insisting that they withhold information that others have a right to know
- ▶ How leaders get information is also a concern
- ▶ Employee e-monitoring



# ACM Code of Professional Ethics



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*

[Digital Library](#) [CACM](#) [Queue](#) [TechNews](#) [Career Center](#)

[Join](#) [Volunteer](#) [myACM](#) [Search](#)

[ABOUT ACM](#) [MEMBERSHIP](#) [PUBLICATIONS](#) [SIGS](#) [CONFERENCES](#) [CHAPTERS](#) [AWARDS](#) [EDUCATION](#) [LEARNING CENTER](#) [PUBLIC POLICY](#) [DIVERSITY & INCLUSION](#)

[Home](#) > [Code Of Ethics](#)

## ACM Code of Ethics and Professional Conduct

### ACM Code of Ethics and Professional Conduct

#### Preamble

Computing professionals' actions change the world. To act responsibly, they should reflect upon the wider impacts of their work, consistently supporting the public good. The ACM Code of Ethics and Professional Conduct ("the Code") expresses the conscience of the profession.

The Code is designed to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. Additionally, the Code serves as a basis for remediation when violations occur. The Code includes principles formulated as statements of responsibility, based on the understanding that the public good is always the primary consideration. Each principle is supplemented by guidelines, which provide explanations to assist computing professionals in understanding and applying the principle.

Section 1 outlines fundamental ethical principles that form the basis for the remainder of the Code. Section 2 addresses additional, more specific considerations of professional responsibility. Section 3 guides individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every ACM member, and principles involving compliance with the Code are given in Section 4.

The Code as a whole is concerned with how fundamental ethical principles apply to a computing professional's conduct. The Code is not an algorithm for solving ethical problems; rather it serves as a basis for ethical decision-making. When thinking through a particular issue, a computing professional may find that multiple principles should be taken into account, and that different principles will have different relevance to the issue. Questions related to these kinds of issues can best be answered by thoughtful consideration of the fundamental ethical principles, understanding that the public good is the paramount consideration. The entire computing profession benefits when the ethical decision-making process is accountable to and transparent to all stakeholders. Open discussions about ethical issues promote this accountability and transparency.

#### On This Page

- Preamble
- 1. GENERAL ETHICAL PRINCIPLES.
  - 1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
  - 1.2 Avoid harm.
  - 1.3 Be honest and trustworthy.
  - 1.4 Be fair and take action not to discriminate.
  - 1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
  - 1.6 Respect privacy.
  - 1.7 Honor confidentiality.
- 2. PROFESSIONAL RESPONSIBILITIES.
  - 2.1 Strive to achieve high quality in both the processes and products of professional work.
  - 2.2 Maintain high standards of professional competence, conduct, and ethical practice.
  - 2.3 Know and respect existing rules pertaining to professional work.
  - 2.4 Avoid and resolve conflicts of interest.

<https://www.acm.org/code-of-ethics>

# ACM Code of Professional Conduct

## PROFESSIONAL LEADERSHIP PRINCIPLES

---

### **1. Ensure that the public good is the central concern during all professional computing work.**

- ▶ people—including users, customers, colleagues, and others affected directly or indirectly— should always be the central concern
- ▶ consider the public good when evaluating the work of a computing professional

### **2. Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.**

- ▶ technical organizations and groups affect broader society, and their leaders should accept the associated responsibilities
- ▶ articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group

### **3. Manage personnel and resources to enhance the quality of working life.**

- ▶ consider the personal and professional development, accessibility requirements, physical safety, psychological well-being, and human dignity of all workers



#### **4. Articulate, apply, and support policies and processes that reflect the principles of the Code.**

- ▶ pursue the organizational policies that are consistent with the Code
- ▶ encourage and reward compliance with those policies
- ▶ take appropriate action when policies are violated

#### **5. Create opportunities for members of the organization or group to grow as professionals.**

- ▶ help group members to improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties
- ▶ opportunities should include experiences that familiarize professionals with the consequences and limitations of particular types of systems



---

## **6. Use care when modifying or retiring systems.**

- ▶ interface changes, the removal of features, and even software updates will affect users' productivity
- ▶ take care when changing or discontinuing support for system features on which people still depend
- ▶ investigate viable alternatives to removing support for a legacy system
- ▶ users should be notified of the risks of continued use of the unsupported system long before support ends



---

## **7. Recognize and take special care of systems that become integrated into the infrastructure of society.**

- ▶ computer systems have the potential to impact society when integrated with everyday activities
- ▶ establish policies for fair system access
- ▶ continually monitor the level of integration of the systems into the infrastructure of society
- ▶ develop the appropriate standards of care when needed



# Ethical Leadership in the Real IT world

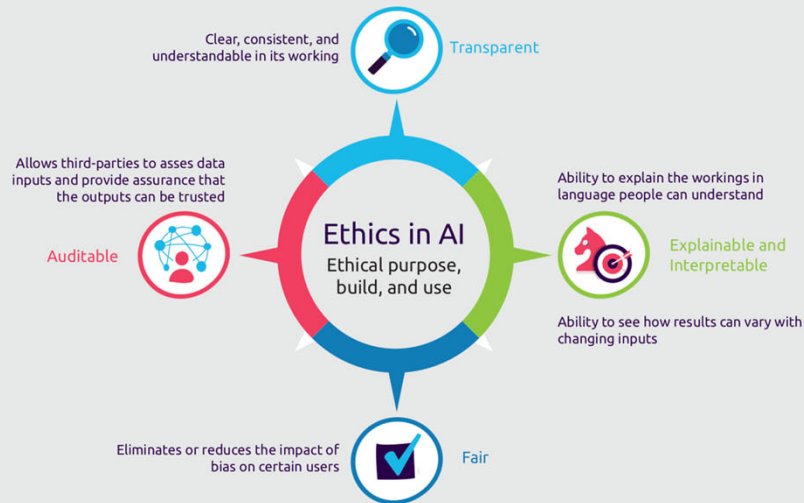
---

- ▶ Is A/B Testing ethical?
- ▶ Is Dark Pattern Design ethical?
- ▶ Persuasion, deception, ambiguity, etc in testing and design
- ▶ What would you do if you are asked by your leader to do these?
- ▶ As a leader, what would you do?

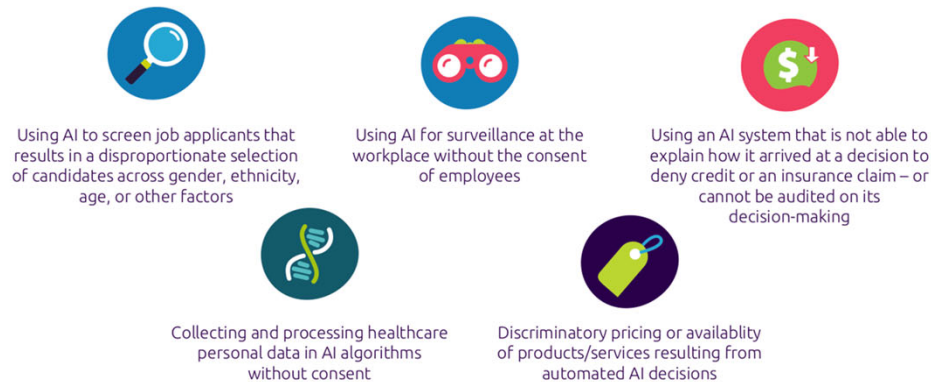


# AI Ethics

## What do we mean by ethics in AI?

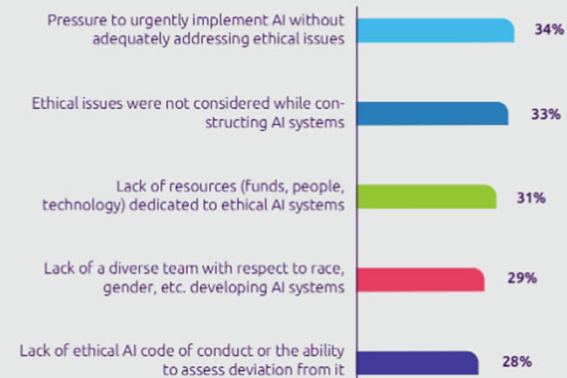


## Examples of ethical issues emerging from the use of AI



## The pressure to implement AI is fueling ethical issues

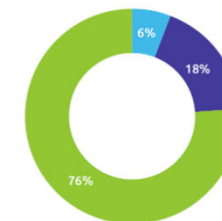
What were the top organizational reasons identified for bias, ethical concerns, or lack of transparency in AI systems? (percentage of executives who ranked the reason in top 3)



Source: Capgemini Research Institute, Ethics in AI executive and consumer survey, N = 1,580 executives, 510 organizations

## Consumers want regulations on the use of AI

Do you think there should be a new law or regulation to regulate the use of AI by organizations?



Source: Capgemini Research Institute, Ethics in AI consumer survey, N = 4,447 consumers.



# AI Governance Framework (by IMDA Singapore)

## 1. internal governance structures and measures

- Adapting existing or setting up internal governance structure and measures to incorporate values, risks, and responsibilities relating to algorithmic decision-making.

## 2. human involvement in AI-augmented decision-making

- A methodology to aid organisations in setting its risk appetite for use of AI, i.e. determining acceptable risks and identifying an appropriate level of human involvement in AI-augmented decision-making.

## 3. operations management

- Issues to be considered when developing, selecting and maintaining AI models, including data management.

## 4. stakeholder interaction and communication

- Strategies for communicating with an organisation's stakeholders, and the management of relationships with them.



# Internal Governance Structures and Measures

- Clear roles and responsibilities for the ethical deployment of AI
  - Responsibility for and oversight of the various stages and activities involved in AI deployment should be allocated to the appropriate personnel or departments.
  - Personnel having internal AI governance functions should be properly trained, and be provided with the resources and guidance needed for them to discharge their duties.

# Internal Governance Structures and Measures

- Risk management and internal controls
  - Using reasonable efforts to ensure that the datasets used for AI model training are adequate for the intended purpose, and to assess and manage the risks of inaccuracy or bias, as well as reviewing exceptions identified during model training.
  - Establishing monitoring and reporting systems as well as processes to ensure that the appropriate level of management is aware of the performance of and other issues relating to the deployed AI.
  - Ensuring proper knowledge transfer whenever there are changes in key personnel involved in AI activities.
  - Reviewing the internal governance structure and measures when there are significant changes to organisational structure or key personnel involved.



- Mastercard is a technology company in the global payments industry. Its global payments processing network connects consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories.
- To achieve its vision, Mastercard leveraged AI in many applications such as:
  - fraud prevention
  - forecasting future spending trends
  - improving user retail experience.
- To ensure robust oversight of Mastercard's use of AI, Mastercard established a Governance Council to review and approve the implementation of AI applications that are determined to be high risk.

# Mastercard

- Mastercard has defined clear roles and responsibilities for the Governance Council. Each representative on the Council brings their expertise to the decision-making process:

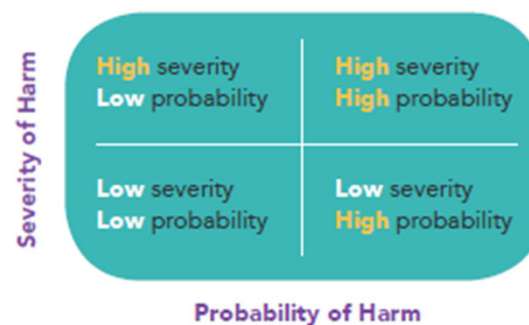
- 
- The diagram is set against a light blue background and lists three roles, each with a purple rounded rectangular box containing the role name. To the right of each role is a description of their responsibilities.
- a. **Chief Data Officer and Chief Privacy Officer** will review the proposal for implementation of AI to ensure that the:
    - Data is fit for purpose for AI;
    - AI is used for an ethical purpose; and
    - Impact to an individual is appropriate and potential harms (including risks to privacy and data protection) are sufficiently mitigated.
  - b. **Chief Information Security Officer** will ensure that security by design is implemented.
  - c. **Data Science teams** that build and implement AI are in continued dialogue with the Data Office and the Privacy Office, so that there is continued information sharing regarding the required governance and the lifecycle of a particular implementation of an AI application.

# Mastercard

- Mastercard has implemented risk management and internal controls to address the risk involved in the AI deployment.
  - conduct initial risk scoring to determine the risk of the proposed AI activity, which includes an evaluation of multiple factors including alignment with corporate initiatives, the data types and sources utilised, and the impact on individuals from AI decisions.
  - identify potential mitigants as part of the process to reduce the level of risk posed by the data being collected or potential biases in the activity.
  - If an AI project has been identified as high risk, it will be referred to the Governance Council for review. Low risk projects will not be subjected to a review and can proceed to the model development stage.

# Determining the level of human involvement in AI-augmented decision-making

- Before deploying AI solutions, organisations should decide on their commercial objectives of using AI, and then weigh them against the risks of using AI in the organisation's decision-making.
- It is also desirable for organisations operating in multiple countries to consider the differences in societal norms, values and/or expectations.
- Organisations' weighing of their commercial objectives against the risks of using AI should ideally be guided by their corporate values.
- It is an iterative and ongoing process, it is desirable for organisations to continually identify and review risks relevant to their technology solutions, mitigate those risks, and maintain a response plan should mitigation fail.



# LEVEL OF HUMAN INVOLVEMENT

A design framework to help determine the degree of human involvement in your AI solution to minimise the risk of adverse impact on individuals.

## SEVERITY AND PROBABILITY OF HARM

LOW

HIGH

### Human-out-of-the-loop

AI makes the final decision without human involvement, e.g. recommendation engines.

### Human-over-the-loop

User plays a supervisory role, with the ability to take over when the AI encounters unexpected scenarios, e.g. GPS map navigations.

### Human-in-the-loop

User makes the final decision with recommendations or input from AI, e.g. medical diagnosis solutions.



# Three broad approaches of human involvement in AI-augmented decision-making

## 1. **Human-in-the-loop**

- human oversight is active and involved, with the human retaining full control and the AI only providing recommendations or input.
- Decisions cannot be exercised without affirmative actions by the human, such as a human command to proceed with a given decision.

## 2. **Human-out-of-the-loop**

- there is no human oversight over the execution of decisions. The AI system has full control without the option of human override.

## 3. **Human-over-the-loop**

- human oversight is involved to the extent that the human is in a monitoring or supervisory role, with the ability to take over control when the AI model encounters unexpected or undesirable events (such as model failure).
- This approach allows humans to adjust parameters during the operation of the algorithm.

## USING THE PROBABILITY-SEVERITY OF HARM MATRIX

An online retail store wishes to use AI to fully automate the recommendation of food products to individuals based on their browsing behaviours and purchase histories. The automation will meet the organisation's commercial objective of operational efficiency.

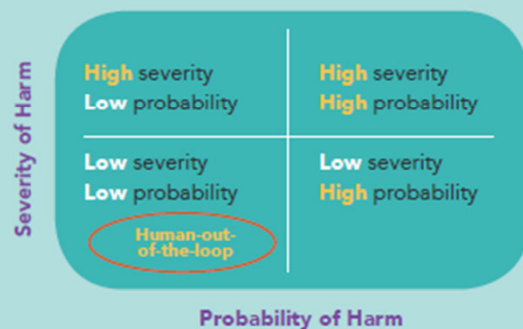


### Probability-severity assessment

The definition of **harm** can be the impact of making product recommendations that do not address the perceived needs of the individuals. The **severity of harm** in making the wrong product recommendations to individuals may be low since individuals ultimately decide whether to make the purchase. The **probability of harm** may be high or low depending on the efficiency and efficacy of the AI solution.

### Degree of human intervention in decision-making process

Given the low severity of harm, the assessment points to an approach that requires no human intervention (i.e. human-out-of-the-loop).



### Regular review

The organisation regularly reviews its approach (i.e. human-out-of-the-loop) to re-assess the **severity** and **probability of harm**, and as societal norms and values evolve.

*Note: This is a simple illustration using bright-line norms and values. Organisations can consider testing this method of determining the AI decision-making model against cases with more challenging and complex ethical dilemmas.*

# More Examples

- **Human-out-of-the-loop.**

- A product recommendation solution may automatically suggest products and services to individuals based on pre-determined demographic and behavioral profiles.
- AI can also dynamically create new profiles, then make product and service suggestions rather than relying on predetermined categories.

- **Human-over-the-loop.**

- A GPS navigation system plans the route from Point A to Point B, offering several possible routes for the driver to pick. The driver can alter parameters (e.g. due to unforeseen road congestions) during the trip without having to re-programme the route.

- **Human-in-the-loop.**

- A doctor may use AI to identify possible diagnoses of and treatments for an unfamiliar medical condition.
- However, the doctor will make the final decision on the diagnosis and the corresponding treatment.



## **Illustration on determining the level of human involvement in AI-augmented decision-making**

- Grab is a Singapore-based company that offers ride-hailing transport services, food delivery and e-payment solutions.
- It uses AI across its platform, from ride allocation, detecting safety incidents, to identifying fraudulent transactions.
- To allocate trips successfully, Grab's AI model considers drivers' preferences based on the following key factors:
  - Driver's preferences for certain trip types
  - Preferred locations where a driver start and end their day
  - Other selective driving behaviors.

# Grab

## Illustration on determining the level of human involvement in AI-augmented decision-making

**Which is the best approach? Human-in-the-loop, human-out-of-the-loop, human-over-the-loop?**

- In determining the level of human involvement in its AI's decision-making for trip allocation, Grab considered the following key factors:
  - The scale of real-time decision-making required. As Grab has to make over 5,000 trip allocations every minute, this would mean an impact to customers in terms of efficiency and cost if a human had to review each trip allocation.
  - The severity and probability to users should the AI model work in a suboptimal manner.
- Grab considered that:
  - it is not technically feasible for a human to make such high volume of trip allocations in a short amount of time
  - there is often little or no harm to life should there be less than optimal trip allocations

# Key Takeaways and Reflection Points from Lecture 9

---

- ▶ What is the scope of IT Risk Management?
  - ▶ How to apply COBIT Risk framework to manage IT risks?
  - ▶ What role should a leader play in Business Continuity Management?
  - ▶ What is crisis leadership and how can IS leaders function effectively to lead the organization out of the crisis?
  - ▶ What are the ethical challenges facing leaders and why are these important (particularly during a crisis)?
  - ▶ What is AI governance and how to apply it to design AI-related governance?
- 

