



# A Practical Approach to TRM Compliance

Sami Benafia

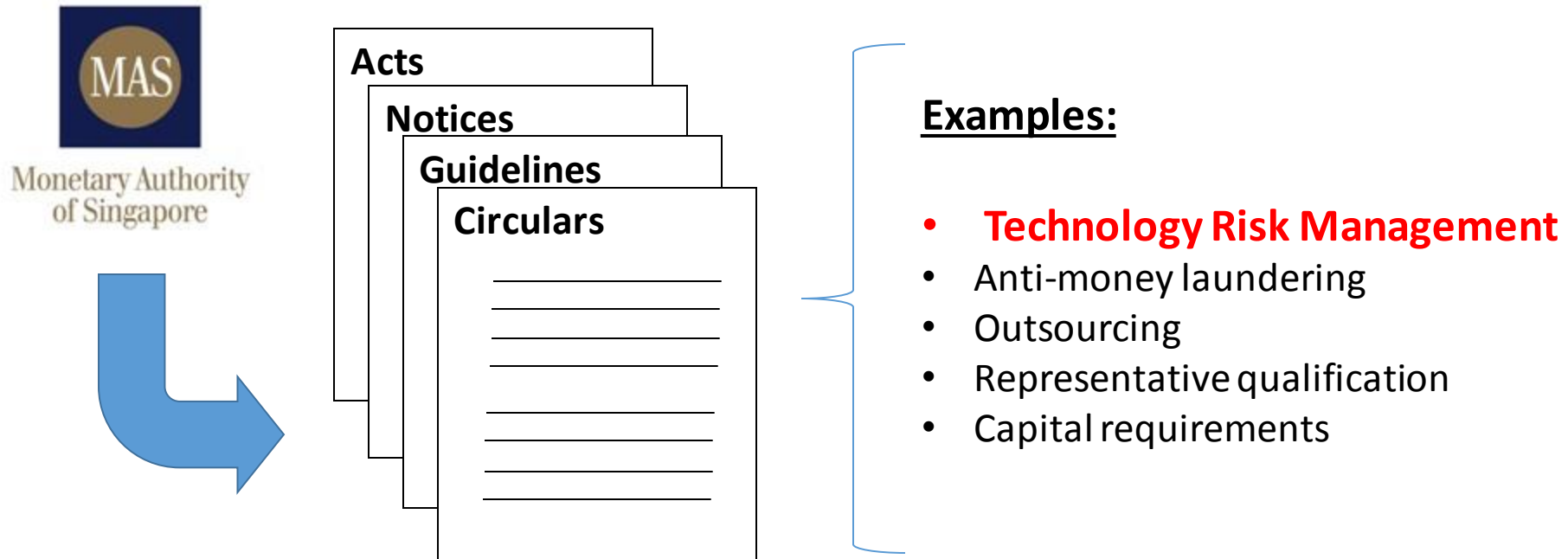
Head of Sales & Marketing



# Agenda

- Introduction
- Data Inventory
- Risk Management
- Incident and Problem Management
- Outsourcing

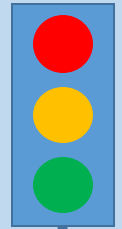
# Introduction to MAS regulations



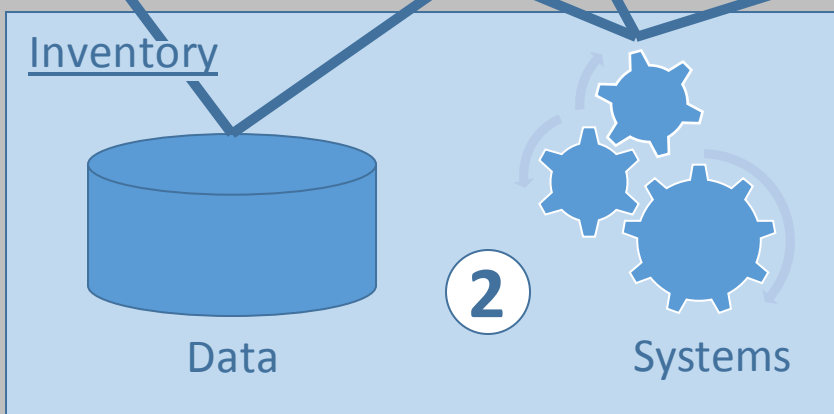
Generally, all FIs (with few exemptions), big or small, are required to comply with the technology regulations set forth in the Notices and Guidelines.

# Business Processes Map

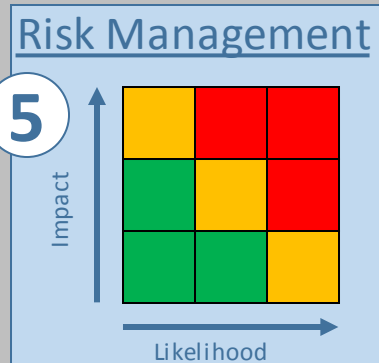
Criticality



**4**  
Incident & Problem Management

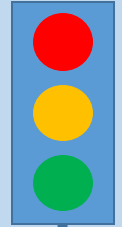


**9**  
Outsourcing



# Business Processes Map

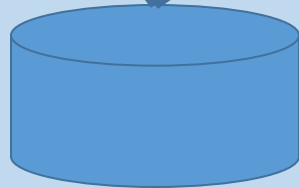
Criticality



**4**  
Incident & Problem Management




Inventory



Data

**2**

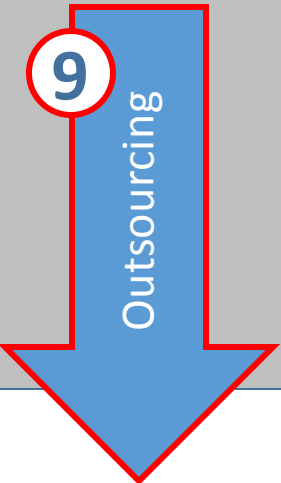


Systems

Classification **3**

- Confidentiality
- Integrity
- Availability

**9**  
Outsourcing



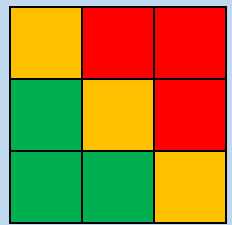
Controls

**6** Access

**7** BCM

**8** Backup

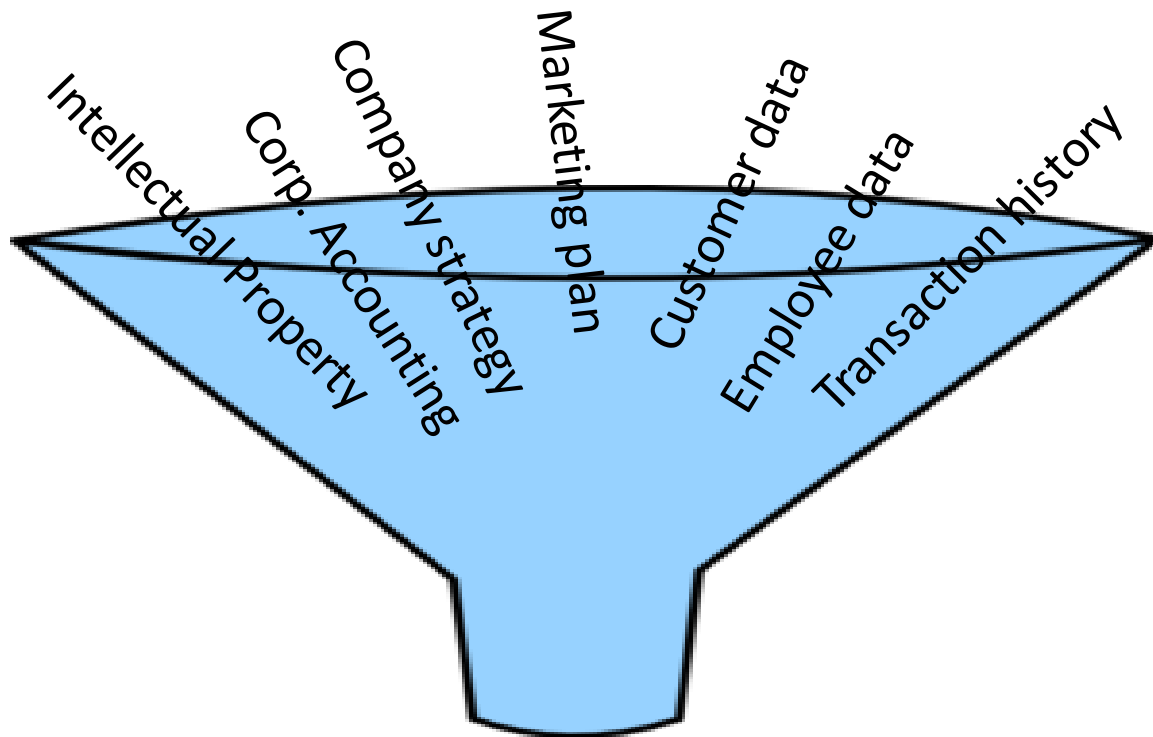
Risk Management **5**



Impact

Likelihood

# What data do I have?



## Key points:

- Know what you need to protect
- Establish data ownership
- Keep inventory updated

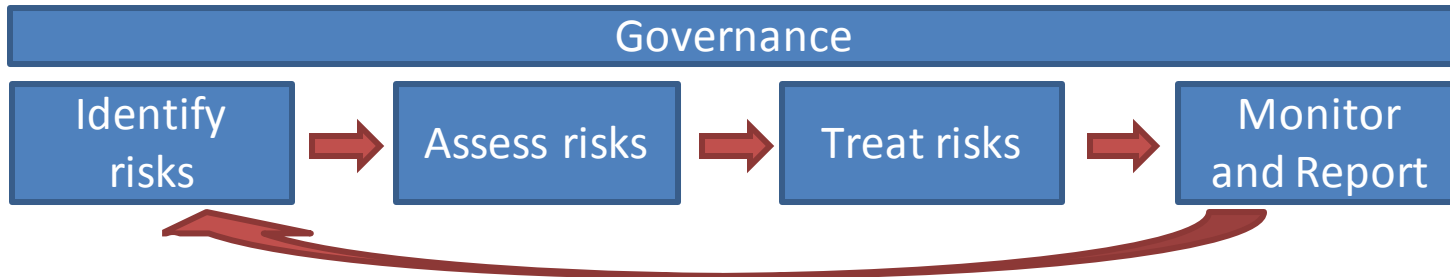
## Data inventory repository

Data	Owner	Location	Custodian	CIA rating	RTO/RPO
KYC	Compliance	KYC DB	RM	High	4h / 8h

# What can go wrong? Am I prepared?



- What can happen to my data that causes harm?
- What is the impact of these potential events?  
How likely will these occur?

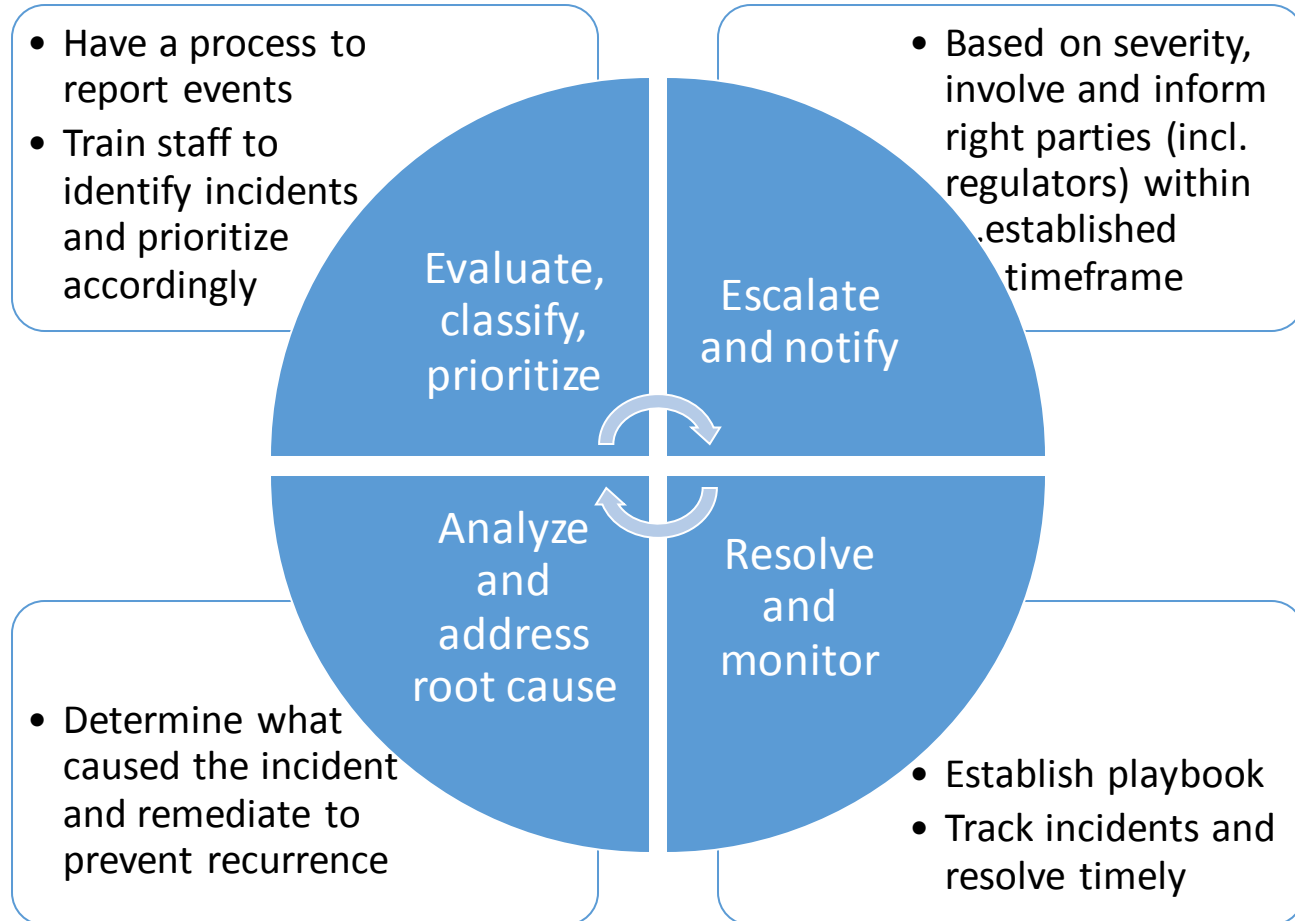


- What safeguards do I have to prevent harmful events from occurring to my data?
- What else can I do to protect my data further?



# Something bad happened! What should I do?

## Incident management framework





# Outsourcing

63%

Breaches traced to third party vendors<sup>1</sup>

\$10 million

Ave. spent responding to third party breaches over prev. 12 months<sup>2</sup>

37% | 73%

Respondents who believe they won't be notified of data breach by third party | N<sup>th</sup> party vendor<sup>3</sup>

Companies suffer financial loss, reputational impact, and regulatory exposure from breaches, even third party breaches. Companies remain liable to its customers and other stakeholders.

**What can I do:**

Limit Access

Monitor performance

Audit/review controls

<sup>1</sup> Soha System's survey on third-party risk management

<sup>2</sup> May 2016 Ponemon report

<sup>3</sup> April 2016 Ponemon report on Data Risk in Third Party Ecosystem



# Thank you!

Sami Benafia

8399 5165

[Sami.Benafia@Ingenia-consultants.com](mailto:Sami.Benafia@Ingenia-consultants.com)

[infosec@Ingenia-consultants.com](mailto:infosec@Ingenia-consultants.com)