Managing Risks to Information

PRUDENTIAL
英國保誠集團

Mike Usher
Director, Information Risk and Privacy, Asia
September 2015

Who am I?

- **Director, Information Risk and Privacy, Asia**
  - 30+ years experience in managing risks to Information and Privacy
    - Governments
    - Telecommunications
    - Financial services
    - Consultancy
  - 15 years working for Prudential
  - 12 years in Asia

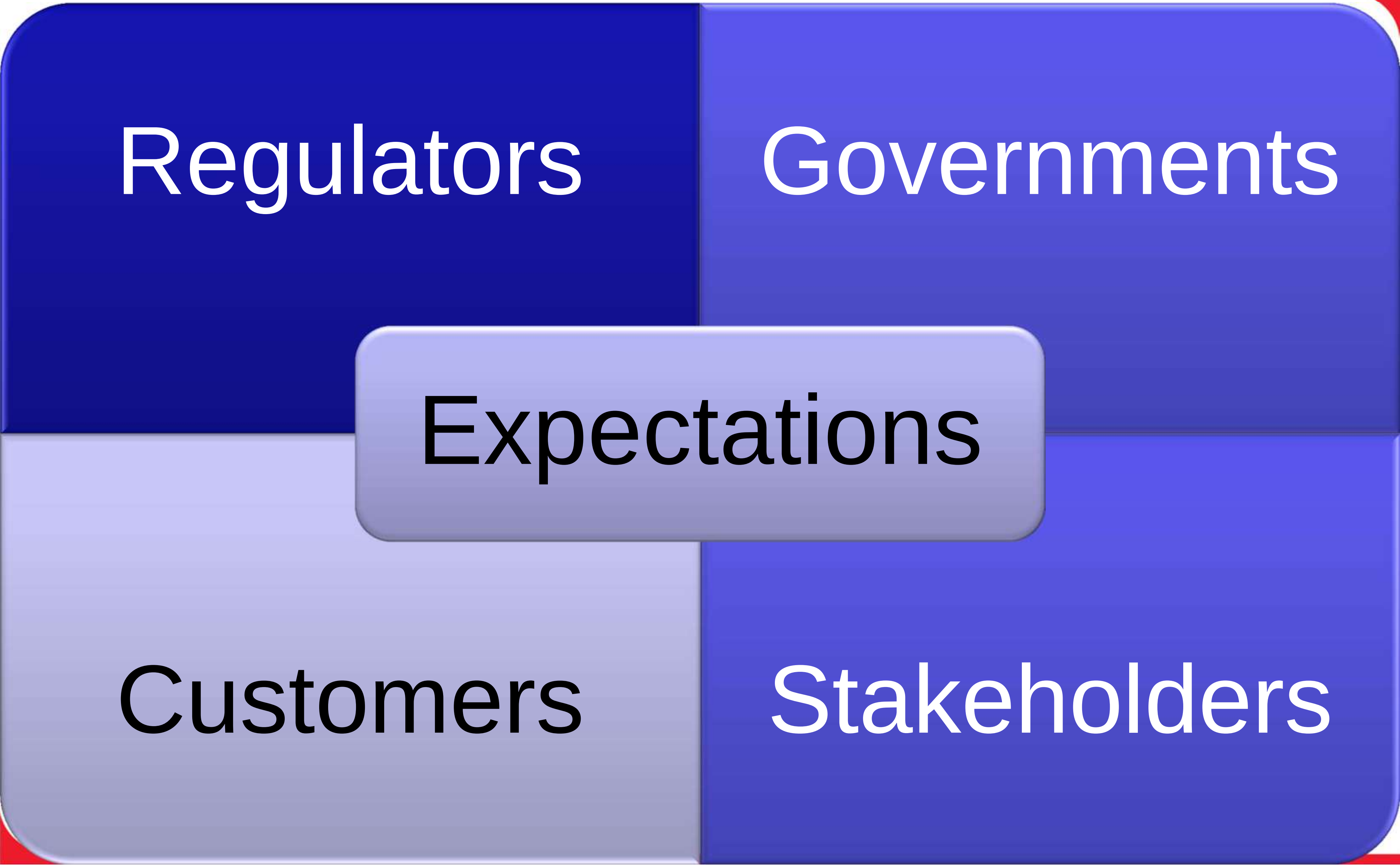
mike.usher@prudential.com.my

What are we protecting?

Raw Material

- Information about
  - Products
  - Customers
  - Staff

Why are we protecting it?



Regulators

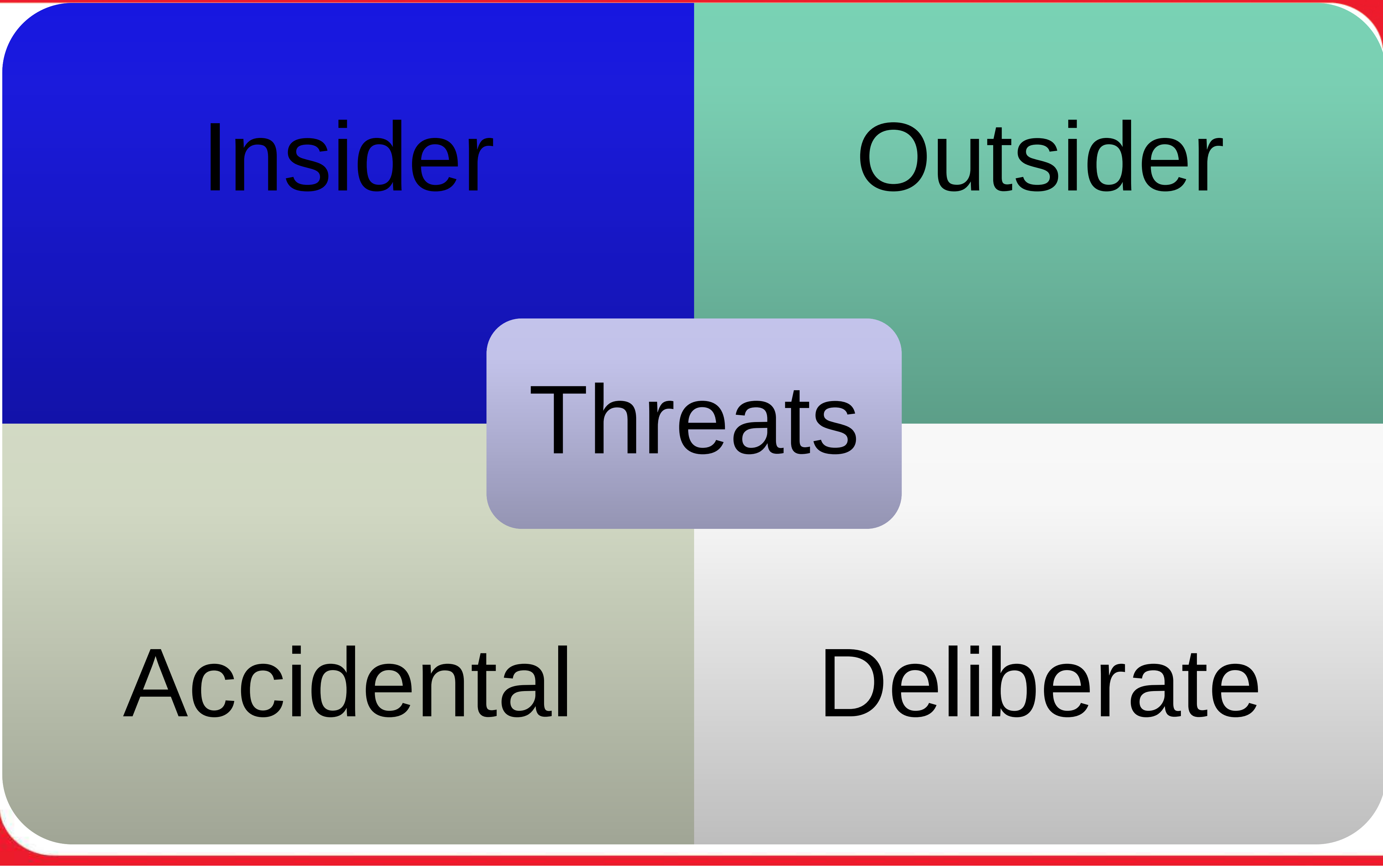
Governments

Expectations

Customers

Stakeholders

What are we protecting it from?



Insider

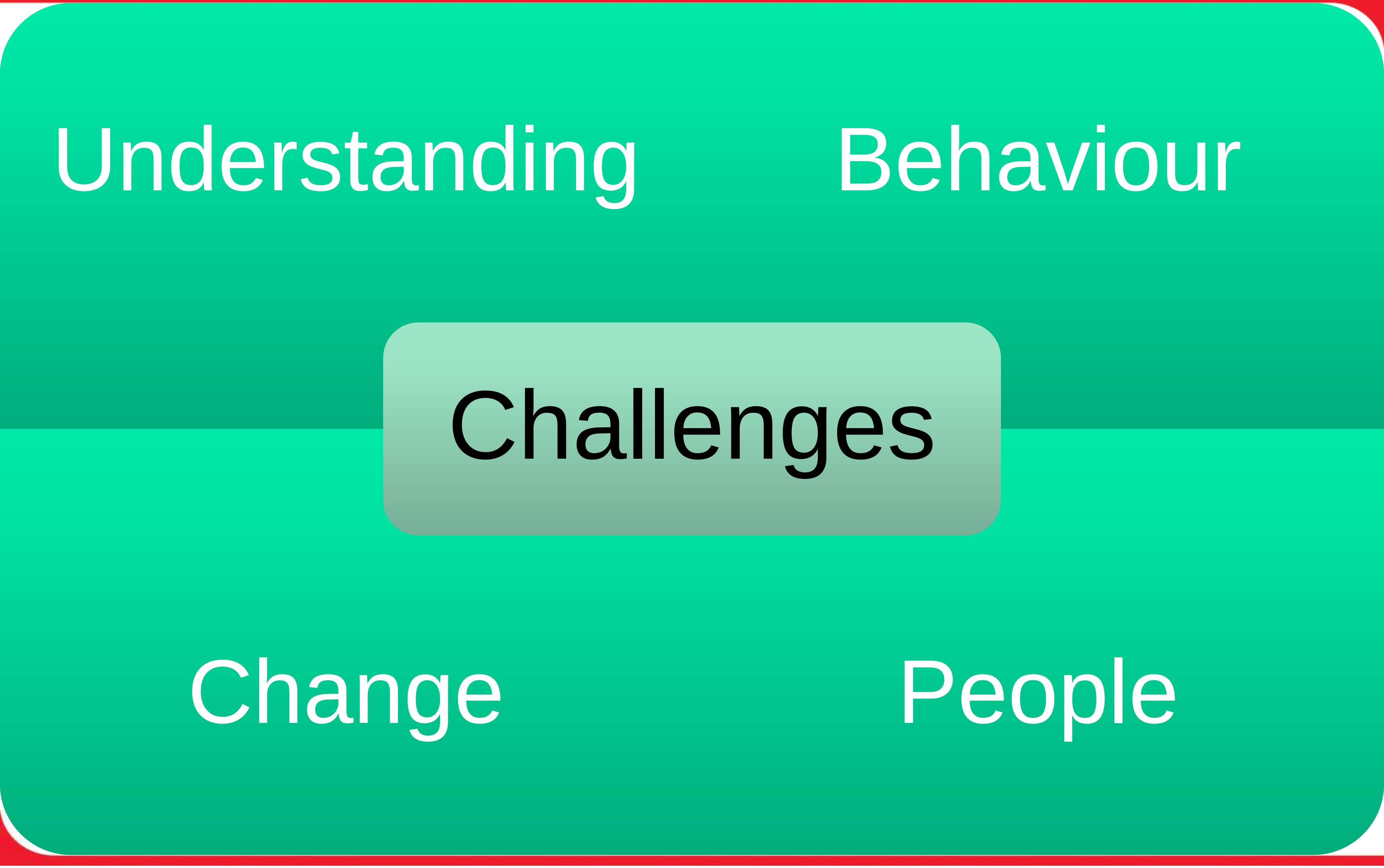
Outsider

Threats

Accidental

Deliberate

Why is it difficult?



Understanding

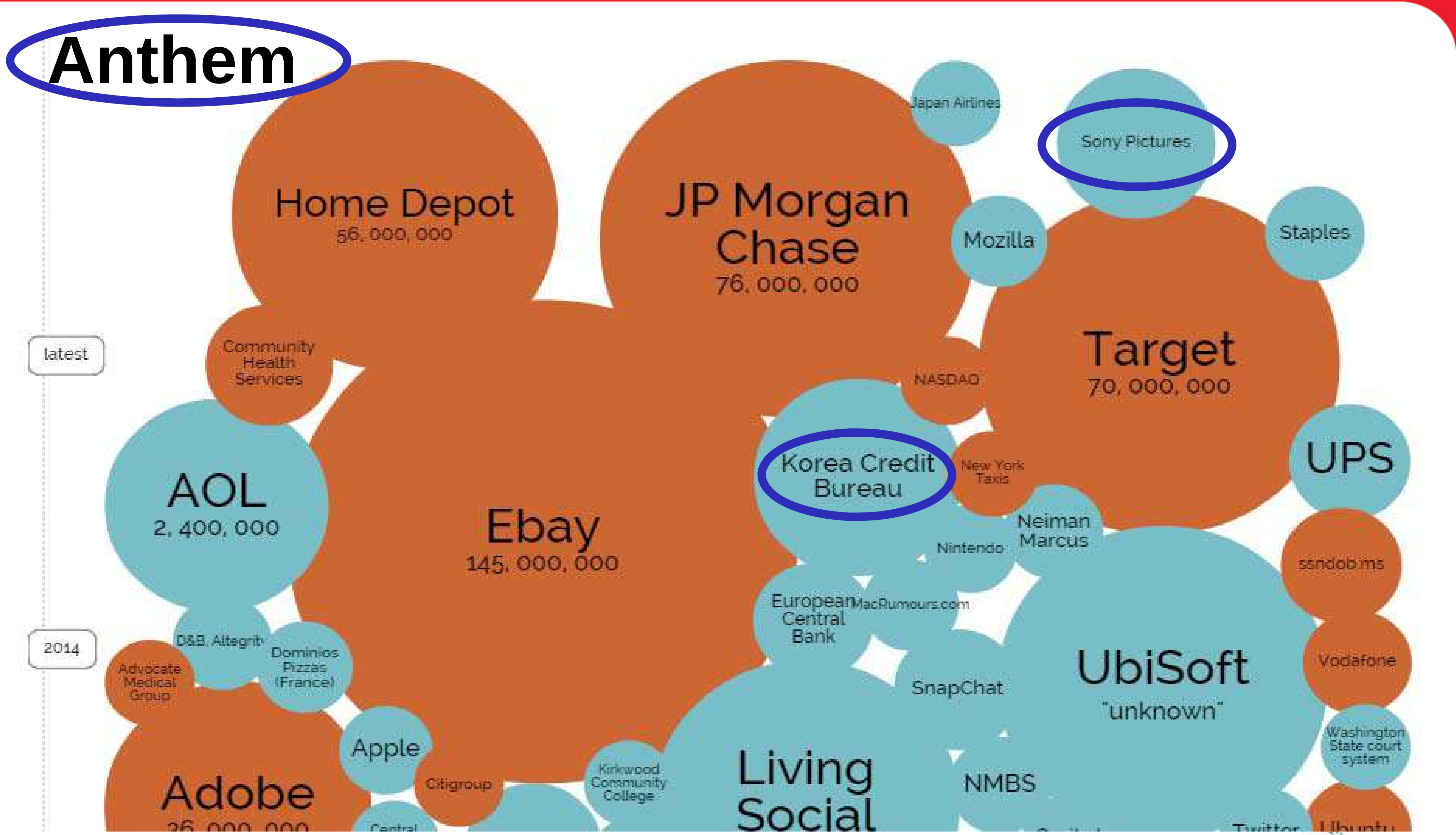
Behaviour

Challenges

Change

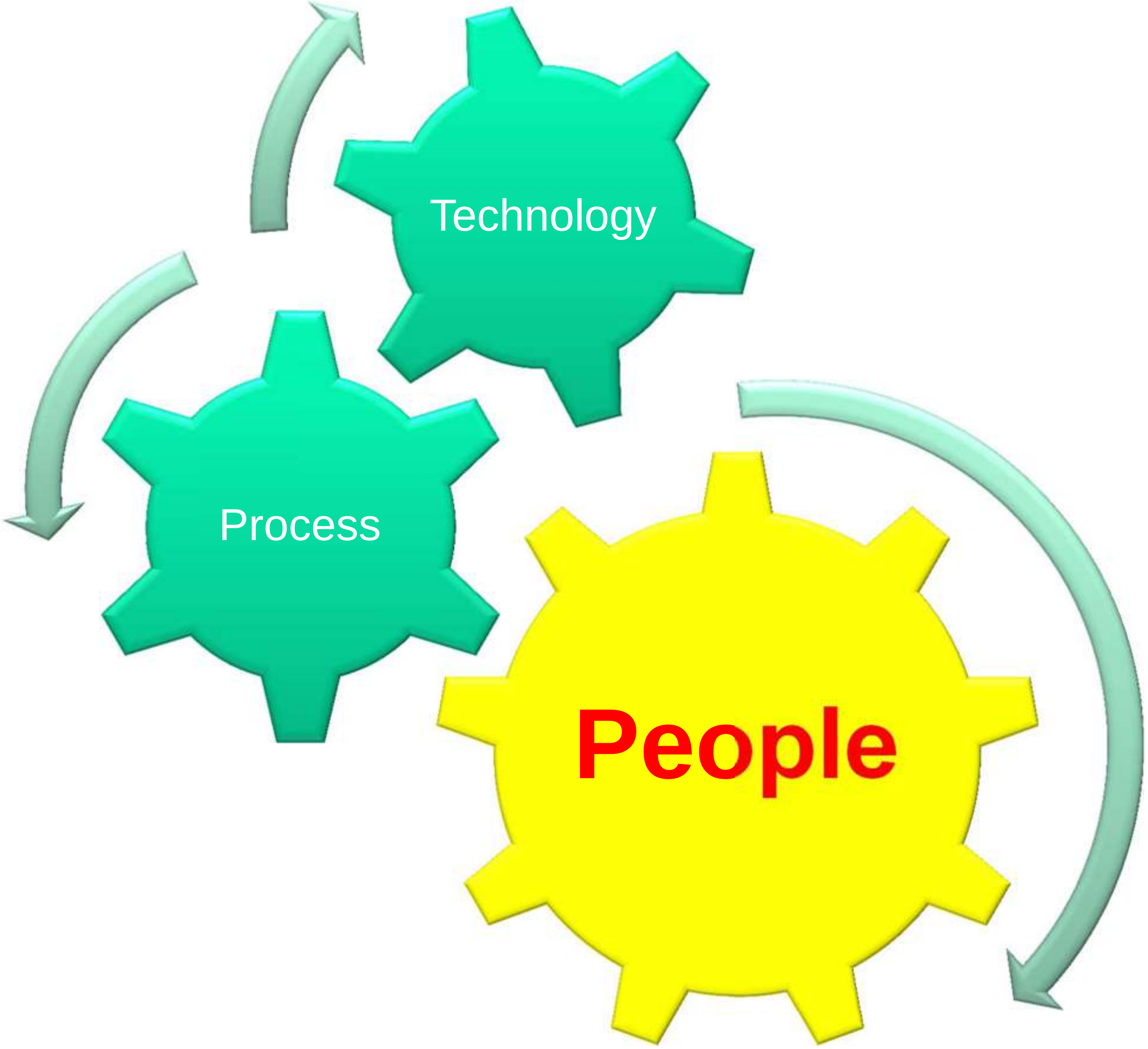
People

"Cyberattacks are growing every day in strength and velocity across the globe!"

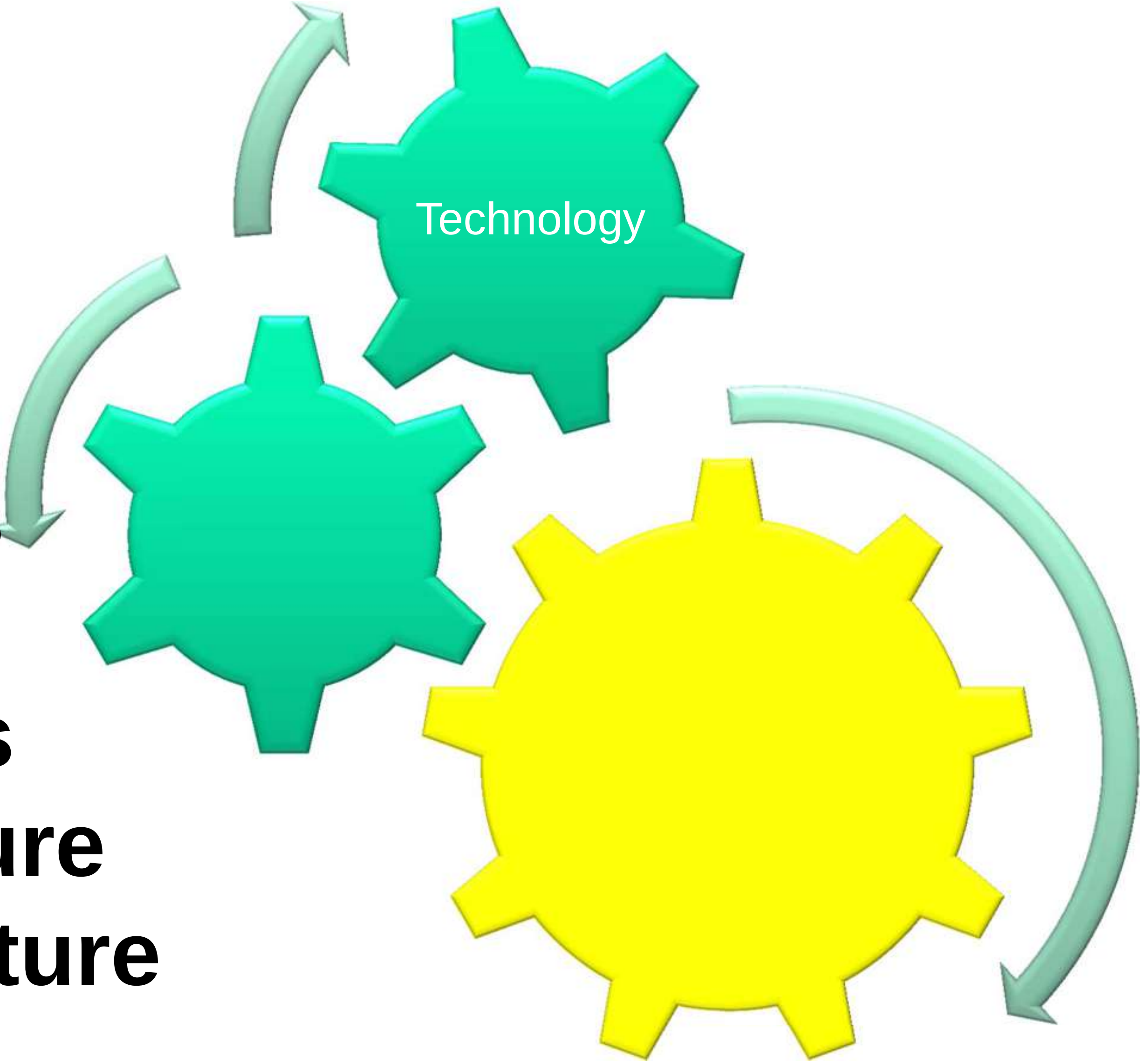


Anthem

Connected pieces

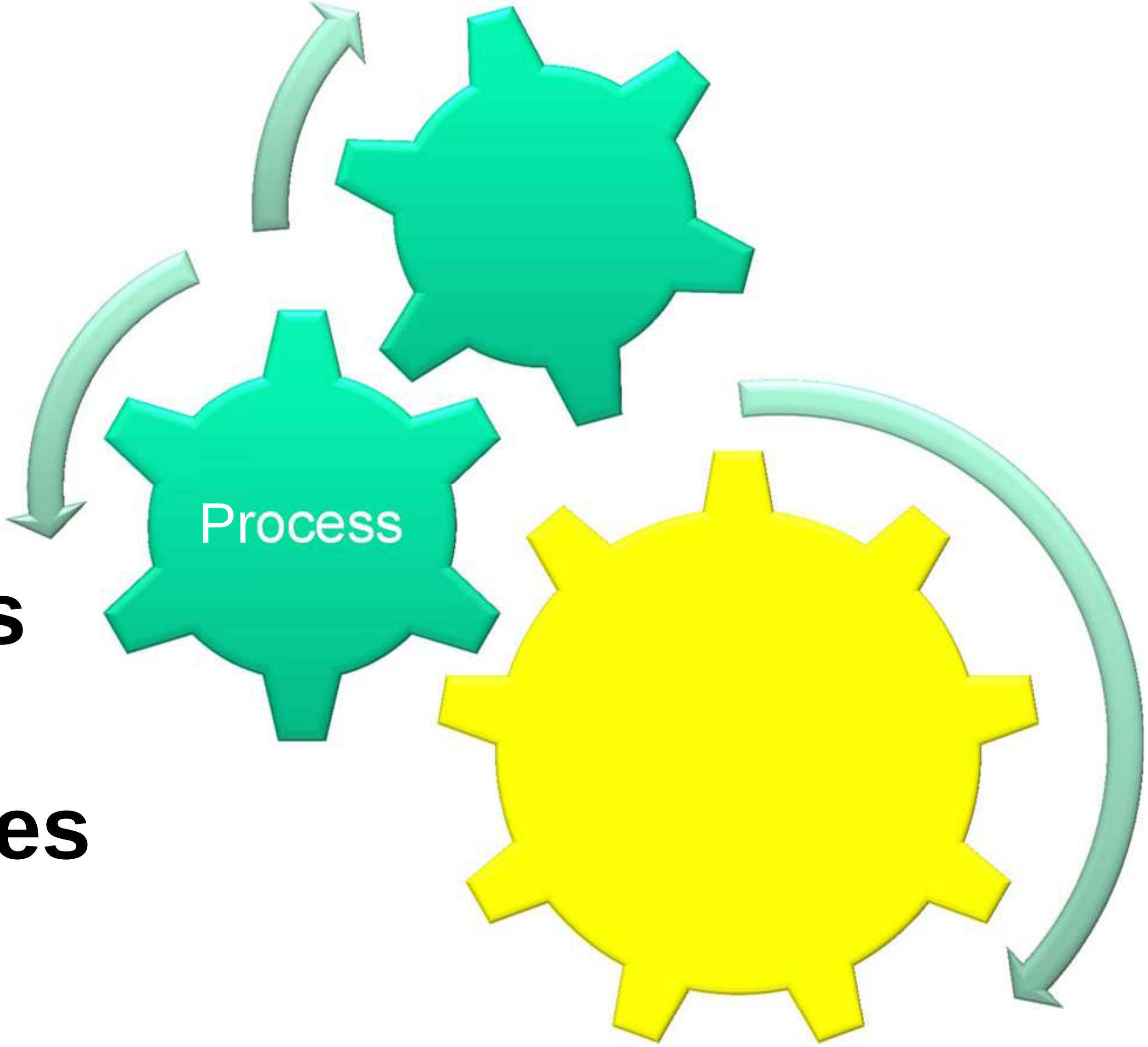


Technology Components



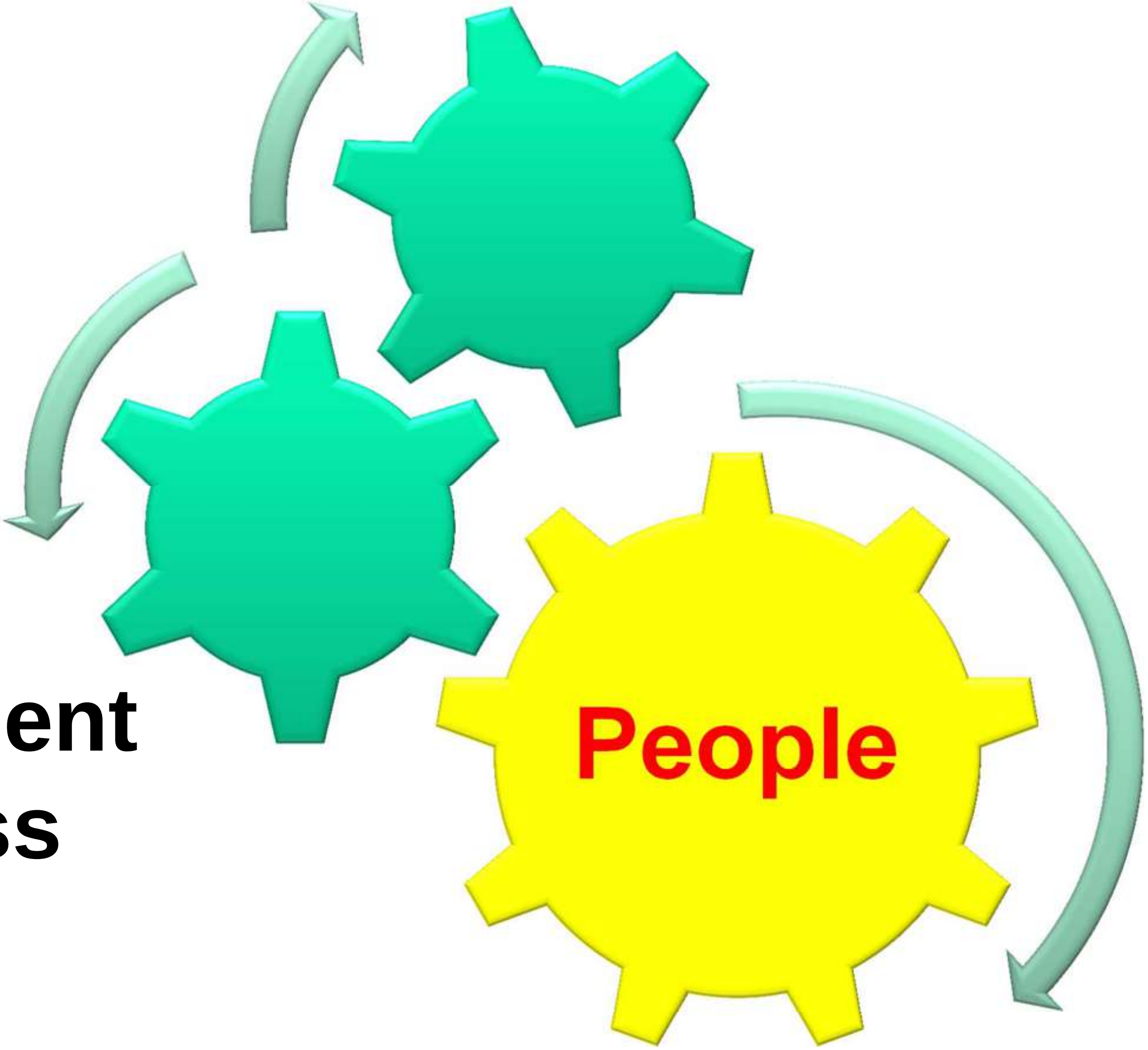
- Principles
- Policies
- Standards
- Architecture
- Infrastructure
- People

Process components



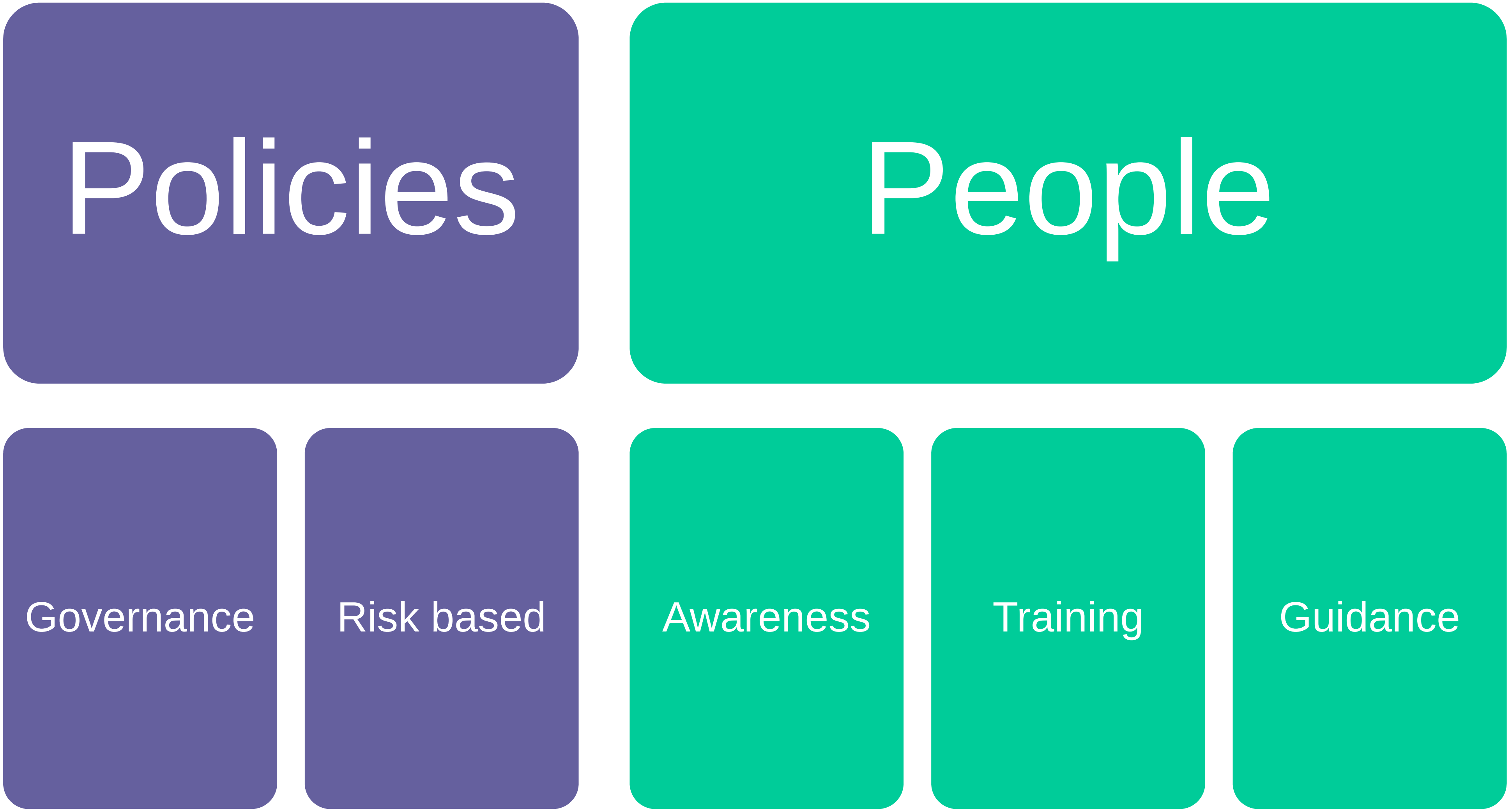
- **Principles**
- **Policies**
- **Procedures**
- **People**

People components



- Management
- Awareness
- Training
- Guidance

Overview



Policies

People

Governance

Risk based

Awareness

Training

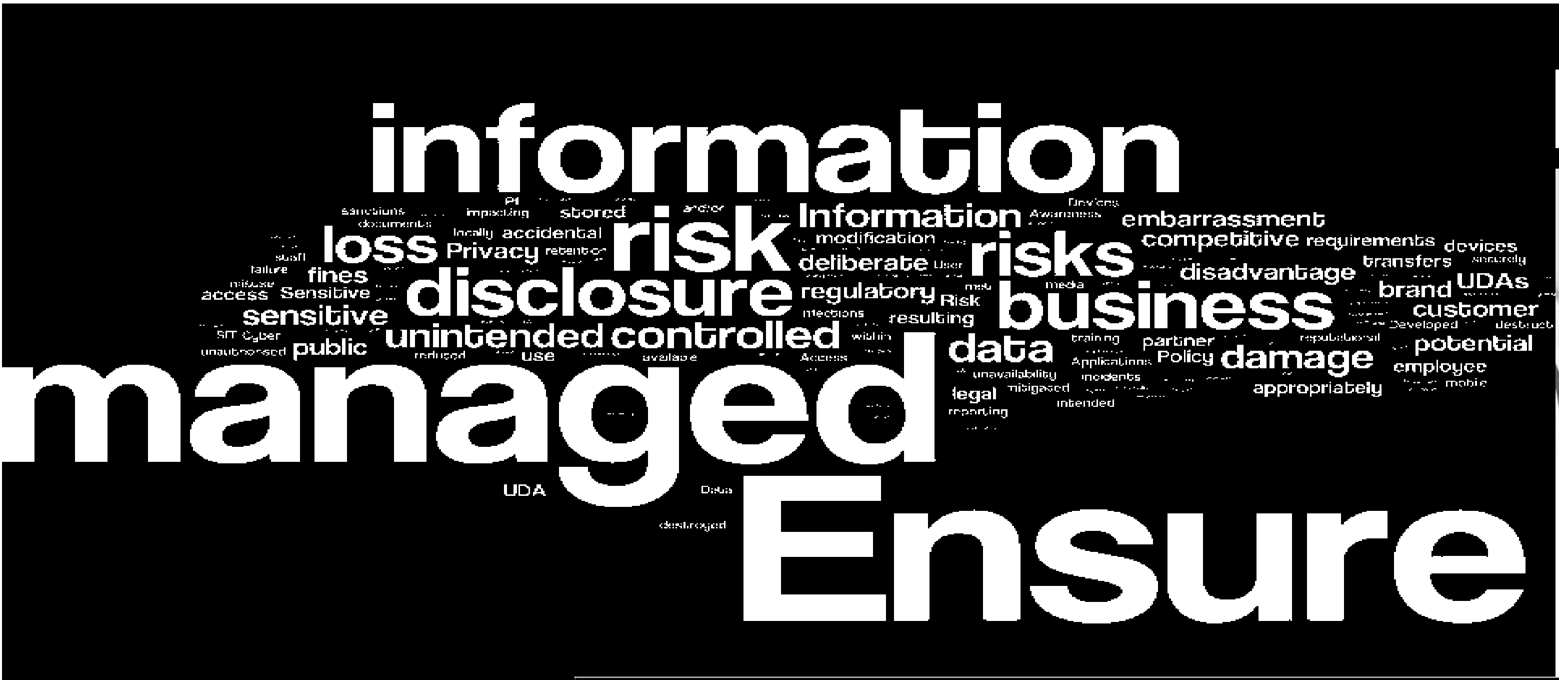
Guidance

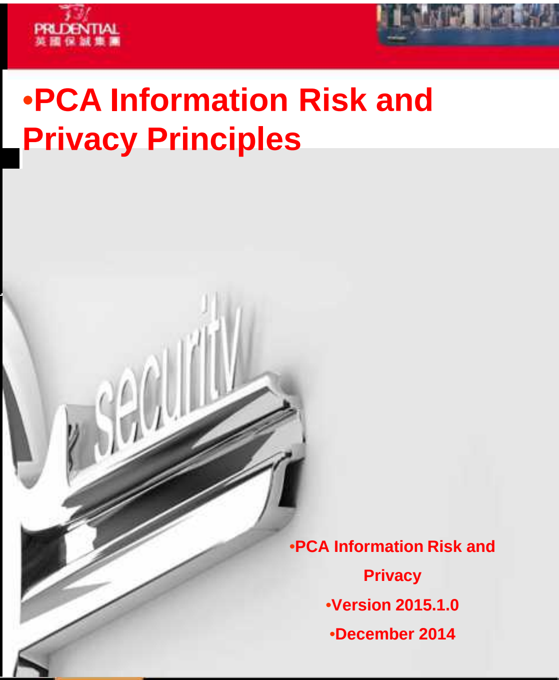
PCA Bestsellers …

Prudential Corporation Asia
IT Security Policy
Prudential Corporation Asia
IT Infrastructure Policy
Prudential Corporation Asia
IT Data Patching Policy
Prudential Corporation Asia
IT Application Development Policy
Procurement Handbook
A handbook to support the procurement of goods and services, including on-going vendor management
PRUDENTIAL
PCA Information Risk and Privacy Policies
SECURITY
PCA Information Risk and Privacy
Version 2015.1.0
December 2014

- Range of policy documents covering different areas
- Work together to provide complete protection to our information across its life

PRUDENTIAL

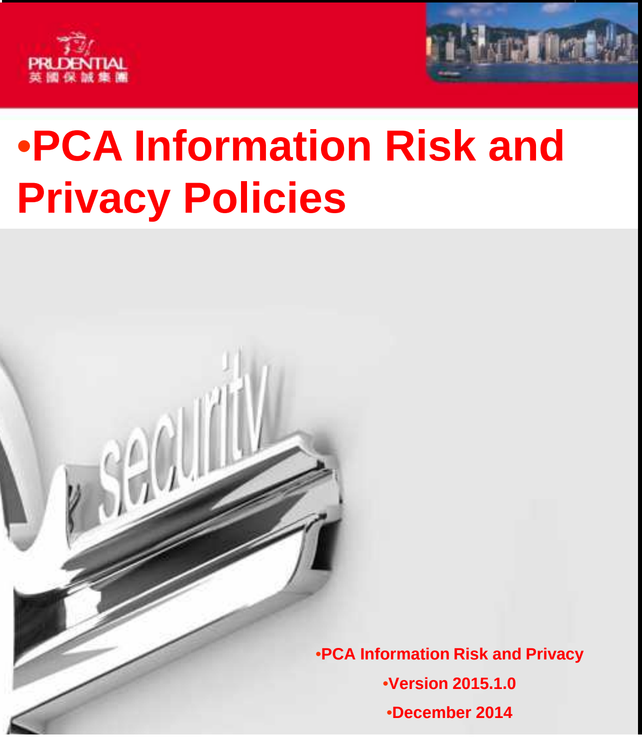



•PCA Information Risk and Privacy Principles

•PCA Information Risk and Privacy

•Version 2015.1.0

•December 2014

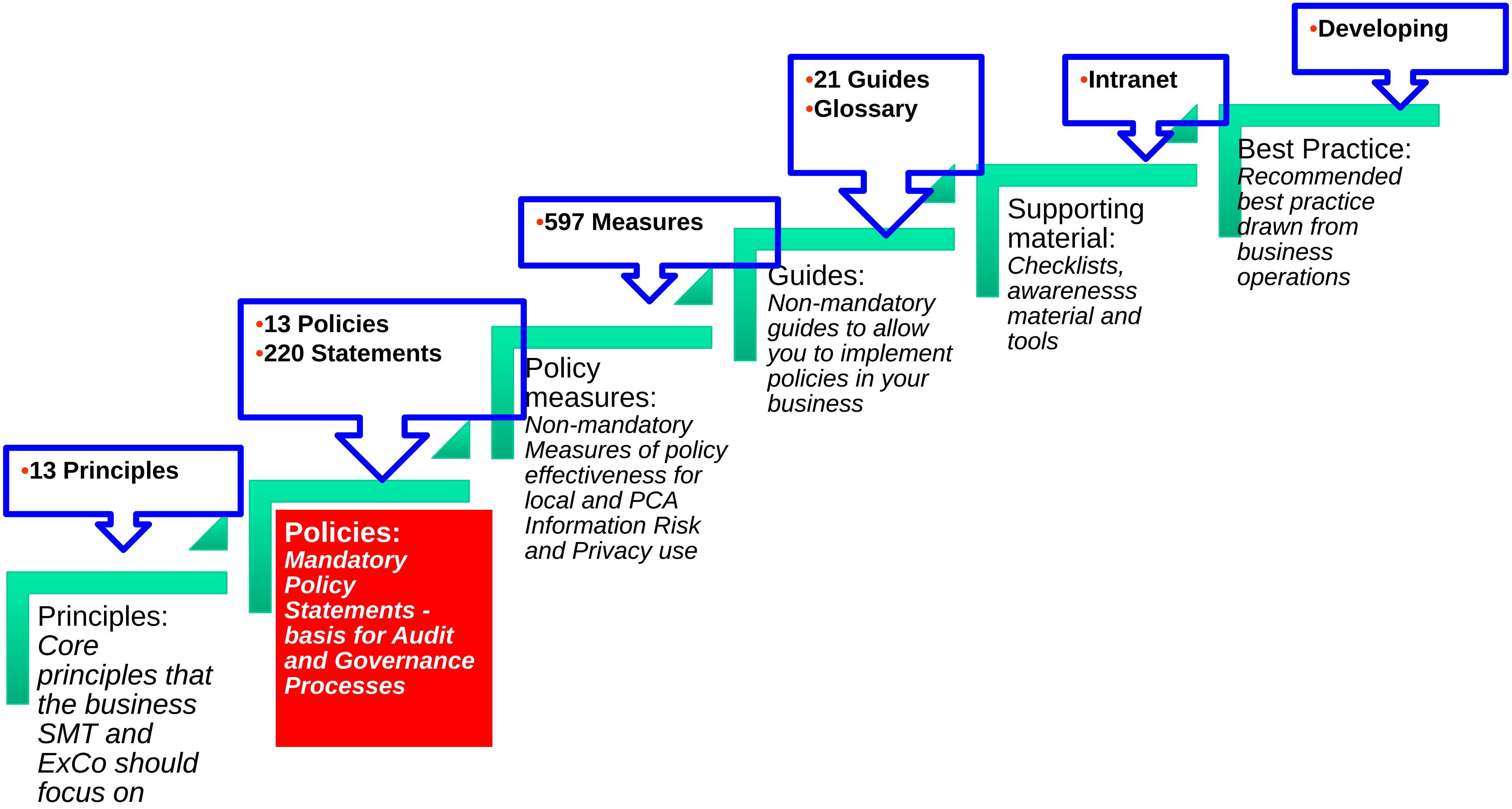

•PCA Information Risk and Privacy Policies

•PCA Information Risk and Privacy

•Version 2015.1.0

•December 2014

Policy structure



- 13 Principles

Principles: *Core principles that the business SMT and ExCo should focus on*

- 13 Policies
- 220 Statements

Policies: ***Mandatory Policy Statements - basis for Audit and Governance Processes***

- 597 Measures

Policy measures: *Non-mandatory Measures of policy effectiveness for local and PCA Information Risk and Privacy use*

- 21 Guides
- Glossary

Guides: *Non-mandatory guides to allow you to implement policies in your business*

- Intranet

Supporting material: *Checklists, awarenesss material and tools*

- Developing

Best Practice: *Recommended best practice drawn from business operations*

The Principles

1. An appropriate management structure is in place.
2. Awareness campaigns and training are conducted
3. Information Risk, Privacy, Cyber and Technology related incidents are reported on a monthly basis both locally and regionally.
4. Processing, storage, transmission and destruction of information is done according to its sensitivity.
5. Personally Identifiable Information (PII) is managed appropriately and in line with local laws and regulations.
6. Sensitive information and physical assets of value are stored and managed securely.
7. Appropriate steps are taken to manage information loss.
8. Access to removable devices and media is controlled and managed.
9. User Developed Applications (UDAs) are controlled and managed.
10. Content available from the internet on internal networks is controlled and managed.
11. Internal and external transfers of sensitive information are controlled and managed.
12. The use of mobile devices is controlled and managed.
13. The storage, retention and destruction of information is controlled and managed.

Areas to consider

- **Sensitive information (e.g. Sony incident)**
  - Understand you need to identify and protect information that would cause harm to your business if something happened
- **Mobile devices (e.g. Japan incident)**
  - Increasing use of smartphones and tablets increase exposure to information loss
- **Removable media (e.g. Korea incident)**
  - Control and manage access to prevent people walking out with your information
- **Shared folders (e.g. “everyone” access)**
  - Think about where information is stored and ensure it is managed wherever it is

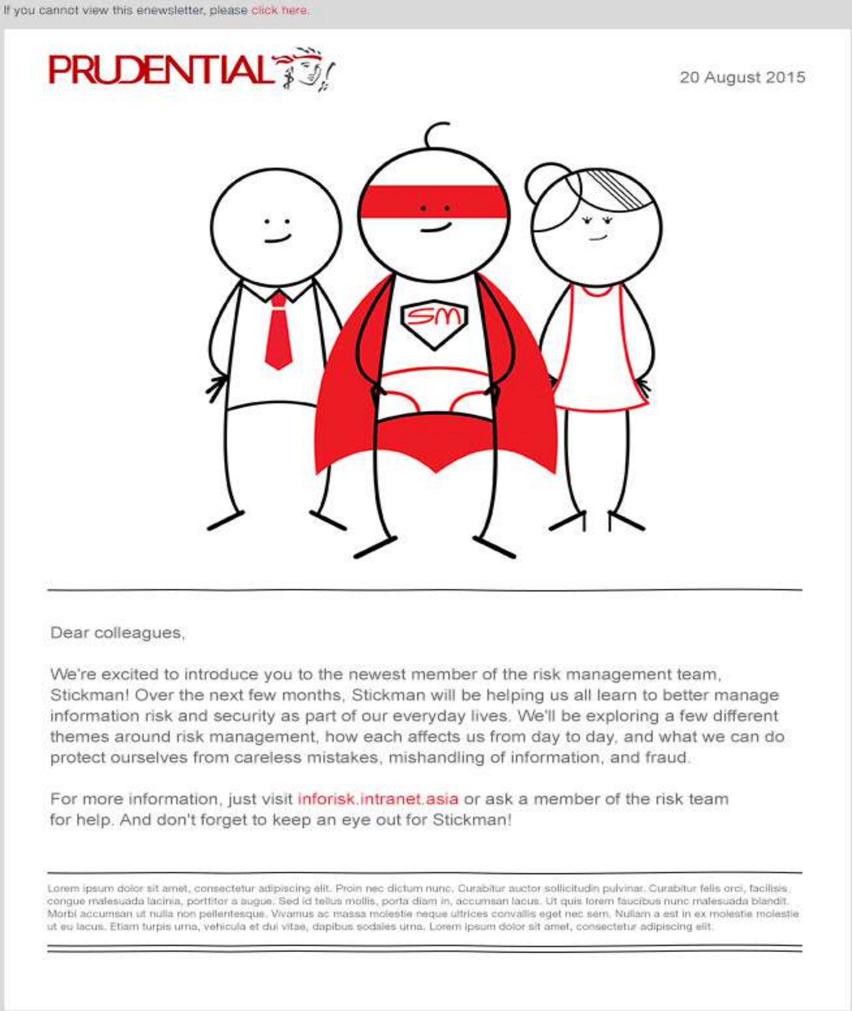
Policy is the first step

- **It starts at the top……**
  - Ownership
  - Accountability
- **Measurement**
  - How well is it implemented?
  - What is happening internally?
  - What is happening externally?

Incidents
Audit findings

- **Governance**
  - Reporting
    - Risk committees
    - C-Level

AWARENESS!!!!!!!



If you cannot view this enewsletter, please click here.

PRUDENTIAL

20 August 2015

Dear colleagues,

We're excited to introduce you to the newest member of the risk management team, Stickman! Over the next few months, Stickman will be helping us all learn to better manage information risk and security as part of our everyday lives. We'll be exploring a few different themes around risk management, how each affects us from day to day, and what we can do protect ourselves from careless mistakes, mishandling of information, and fraud.

For more information, just visit inforisk.intranet.asia or ask a member of the risk team for help. And don't forget to keep an eye out for Stickman!

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin nec dictum nunc. Curabitur auctor sollicitudin pulvinar. Curabitur felis orci, facilisis congue malesuada lacinia, porttitor a augue. Sed id tellus mollis, porta diam in, accumsan lacus. Ut quis lorem faucibus nunc malesuada blandit. Morbi accumsan ut nulla non pellentesque. Vivamus ac massa molestie neque ultrices convallis eget nec sem. Nullam a est in ex molestie molestie ut eu lacus. Etiam turpis urna, vehicula et dui vitae, dapibus sodales urna. Lorem ipsum dolor sit amet, consectetur adipiscing elit.

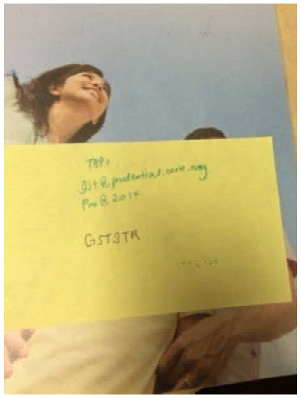
Awareness and training

Most incidents and internal audit findings are caused by people……………….

Don’t forget simple things

PII not shredded

Payment information not secure

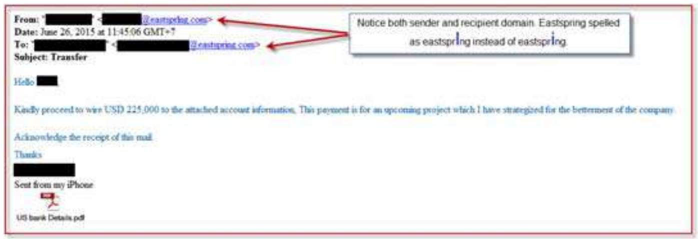


Passwords

Removable media

Transfers

Phishing and Social Engineering



From: "[redacted]" <[redacted]@eastsprlng.com>
Date: June 26, 2015 at 11:45:06 GMT+7
To: "[redacted]" <[redacted]@eastsprlng.com>
Subject: Transfer

Hello [redacted]

Kindly proceed to wire USD 225,000 to the attached account information. This payment is for an upcoming project which I have strategized for the betterment of the company

Acknowledge the receipt of this mail

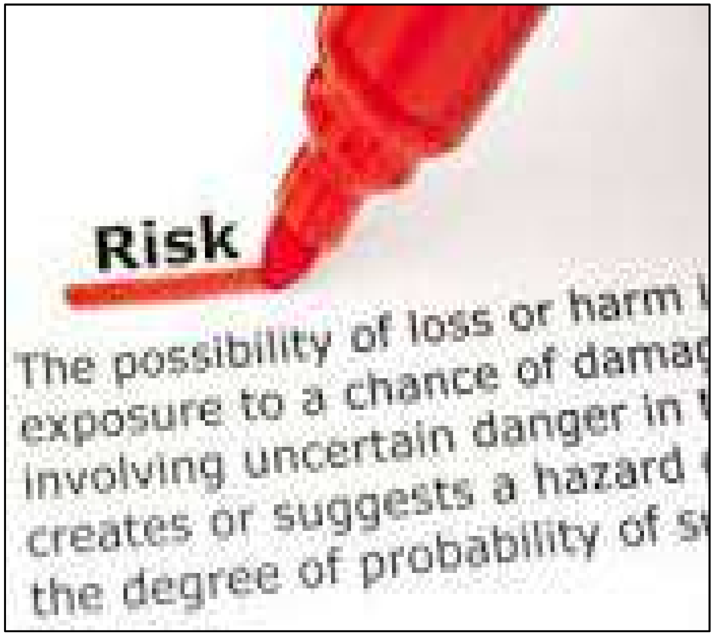
Thanks

[redacted]

Sent from my iPhone

US bank Details.pdf

Notice both sender and recipient domain. Eastspring spelled as eastsprlng instead of eastspring.


Risk
The possibility of loss or harm
exposure to a chance of damag
involving uncertain danger in
creates or suggests a hazard
the degree of probability of s