金融數位化時代下的資訊風險與控制管理

PROMETHEUS YANG, CISA, CISM, CRISC, CFE, ISO27001 LA

國際產業安全協會(ASIS)台灣分會會長
WHY DO CARS HAVE BRAKES?

為什麼汽車需要有煞車？
WHY SHOULD ORGANIZATION MANAGE IT RISK?
為什麼企業需要管理資訊風險?

• 對資訊系統仰賴程度提高
• 組織資源有限
• 所處的環境越來越複雜
1995 – 1999
Internet Startup

2000 – 2003
E-commerce

2004 – 2007
Extended Enterprise

2008 – 2012
Borderless Enterprise

2013 – 2018
Cloud, IoT, Big Data, AI

Increasing CyberCrime

Increasing IT Outsourcing Trend

Increasing Online Fraud

Payment Card Security Standard

Mobile

Cloud Computing

IoT & Big Data

Home Depot Target Data Breach

Obama Cybersecurity Executive Order

2016 US Presidential Election Influence

SWIFT Heist

Evolving Business Model

Emerging Threats

Increasing Regulatory Requirements

Major Damage Incidents Through Intrusions (virus, worms, DOS)

Increasing Identity Theft

Mobile

Cloud Computing

IoT & Big Data

Home Depot Target Data Breach

Obama Cybersecurity Executive Order

2016 US Presidential Election Influence

SWIFT Heist

Evolving Business Model

Emerging Threats

Increasing Regulatory Requirements

Increasing IT Outsourcing Trend

Increasing Online Fraud

Payment Card Security Standard

Mobile

Cloud Computing

IoT & Big Data

Home Depot Target Data Breach

Obama Cybersecurity Executive Order

2016 US Presidential Election Influence

SWIFT Heist
- Internal and External Malicious Threats
- IT Policy and External Regulations
- Application and IT Performance

- Natural Disaster and System Failure
- IT Policy and External Regulations
- Application and IT Performance

IT RISK MANAGEMENT
資訊風險管理

VS.

IT SECURITY MANAGEMENT
資訊安全管理
WHICH COMPANIES HAVE TECHNOLOGY RISK MANAGEMENT FUNCTION?

哪些企業已設有資訊風險管理專責單位?
HOW CAN COMPANIES BENEFIT FROM IT RISK MANAGEMENT?

資訊風險管理能為企業帶來哪些好處？

• 降低資訊風險發生機率與影響
• 有效跨部門溝通資訊風險
• 協助資訊風險控制活動化繁為簡
• 落實三道防線精神
WHAT ARE THE COMMON TECHNIQUES USED FOR IT RISK MANAGEMENT?
實用的資訊風險管理技巧有哪些?

• Risk and Control Matrix, RCA (風險管理矩陣);
• Self-assessment (自行查核);
• Risk Register (風險註冊);
WHAT RESOURCES CAN HELP YOU ESTABLISH IT RISK MANAGEMENT FUNCTION?

哪些資源可協助建立資訊風險管理機制?
MANAGE RISK AND CONTROLS THROUGH PARTICIPATION AND PARTNERSHIP
The End
APPENDIX. 補充說明
HOW TO ESTABLISH RISK AND CONTROLS MATRIX?

如何建置風險控制矩陣？
Define Scope
定義範圍

Identify Risk
辨識風險

Design Controls
設計控制

Monitor Risk
監控風險

Review Risks and Control
定期覆核

定期覆核
### RISK IDENTIFICATION

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Sub Process</th>
<th>Global Process Owner</th>
<th>Risk Owner</th>
<th>Global OR Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential Failure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gross Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PF Context</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Sub-Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gross Risk</td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
</tbody>
</table>

#### Identify Causes

<p>| Causes | |
|--------||</p>
<table>
<thead>
<tr>
<th>Control #</th>
<th>Control Description</th>
<th>Control Owner</th>
<th>Population Size</th>
<th>Cause #</th>
<th>Control Type</th>
<th>Frequency</th>
<th>Control Indicator #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### TRACKING & MONITORING TECHNIQUES
追蹤與監控技巧

<table>
<thead>
<tr>
<th>Control Indicator #</th>
<th>Control Indicator Type</th>
<th>Control Indicators Description</th>
<th>Control #</th>
<th>Frequency</th>
<th>Measurement Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>KCI / KRI / CST</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>