

# Biometric Compliance in Financial Services

Adhering to financial industry regulations when using Biometric authentication

# Agenda

**01**

Identity Frauds &  
Deepfake Impact

**02**

Evolving Regulatory  
Landscape

**03**

Biometric Risks  
& Safeguards

**04**

How Deloitte  
Can Help

# 01

## Identity Frauds & Deepfakes Impact in the Banking and Payment Services Sector



## Biometrics Definition & Classification

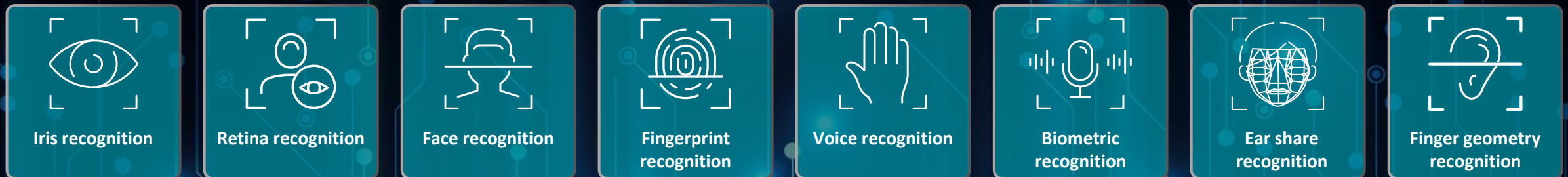
According to the definition from the **National Institute of Standards and Technology (NIST)**, **biometrics** are **automated identification methods** that use a **person's behavioural or physiological characteristics** to **verify their identity**.

GDPR Article 4 (14) states that **biometric data** means **personal data** resulting from **specific technical processing** relating to the **physical, physiological or behavioural characteristics** of a **natural person**, which **allow or confirm the unique identification** of that **natural person**, such as **facial images** or **dactyloscopic data**.

- In addition, GDPR classifies Biometric data as 'sensitive personal information' and 'special categories of personal data' that requires extra care in the storage and protection of the data.*

Specifically, sensitive PII data should be containerized, segregated and stored separately to ensure increased data protection and cyber security robustness.

### Examples of physiological biometrics include:



# What Businesses Need to Know About Deepfakes, Synthetic Identity, Biometric Fraud & Identity Theft

Deepfakes are digitally manipulated videos/images of a person's face altered to appear as someone else. With the advancement of generative artificial intelligence (AI), and machine learning (ML) tools, deepfakes and synthetic identity are becoming more sophisticated and difficult to distinguished.

## Face Swaps



Use of AI to morph and blend the source face into a target face

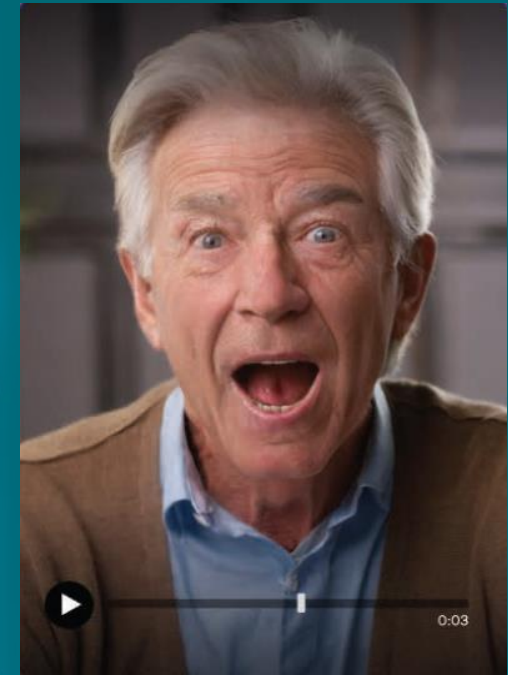
Source: Onfido Identity Fraud Report 2024

## AI generated images



A new synthetic identity created with a realistic face by generative AI entirely from scratch

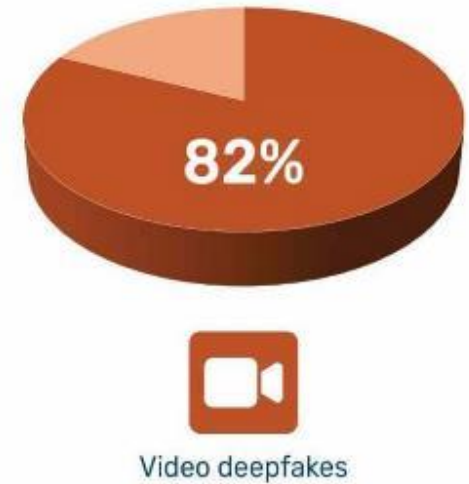
## Lip-sync videos



An original person with lips manipulated with deepfake voice to say something different from the original video

# Deepfake Technology Manipulation Landscape

Deepfakes have been ranked as the top risk and most worrying uses of AI, according to the report by the World Economic Forum in 2023 and deepfakes worldwide incidents in the Fintech sector have reported to increase 700% in 2023 from the previous year.



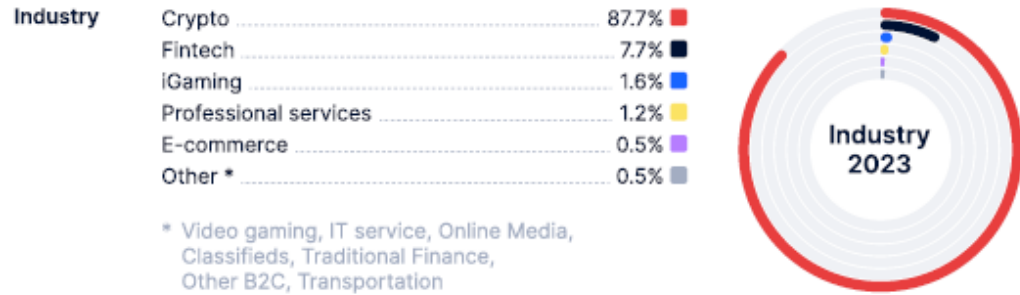
It is predicted that as much as 90% of online content may be synthetically generated by 2026.

The risks faced by individual users and corporate entities are severe, and WEF reports that the Banking, financial services and Insurance sector is particularly impacted by the compounding risks of deepfake scams and identity theft in fraudulent misuse in services, such as personal banking and payments.

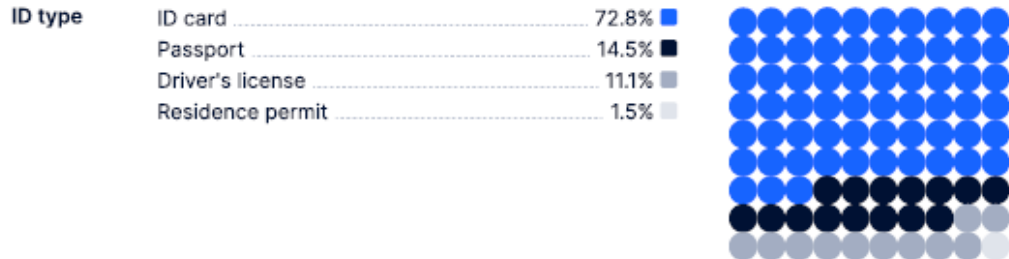
# Urgency to Address Identity Fraud in the APAC & Thailand Region

Economic Forum has ranked disinformation as one of the top risks in 2024, and deepfakes have been ranked as one of the most worrying uses of AI.

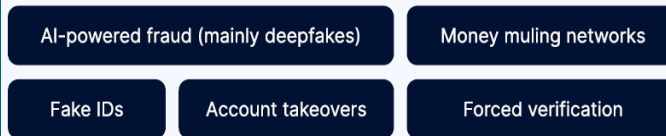
## Deepfake fraud by industry, 2023



## Fraud percentage by identity document type, 2023



## Top 5 identity fraud types



Two additional identity fraud trends have emerged in 2023:  
 Account takeovers (+155% YoY)  
 Forced verification (+305% YoY)

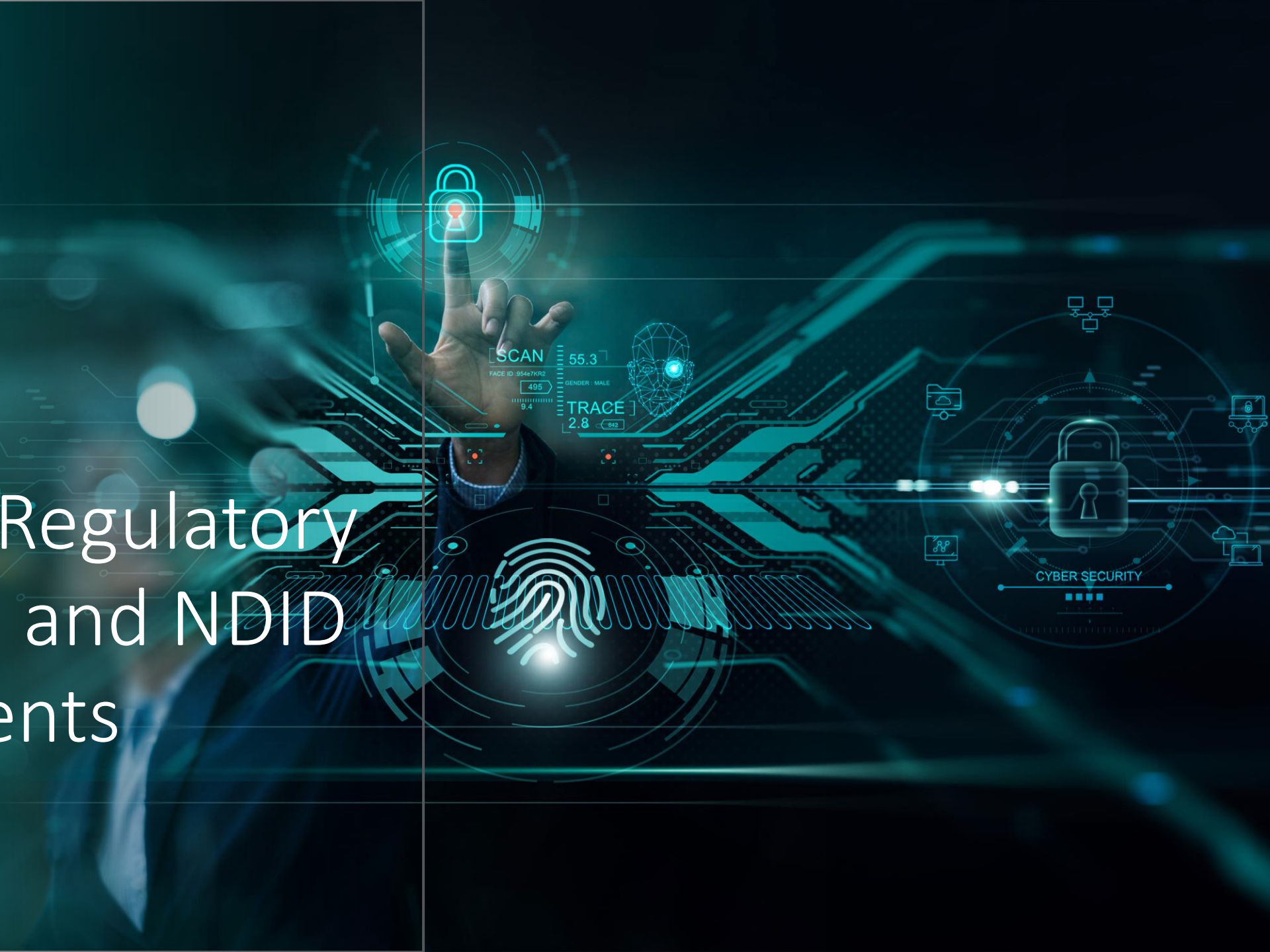
## Growth in the number of deepfakes in APAC, 2022-2023



Source: Sumsb Identity Fraud Report 2023

# 02

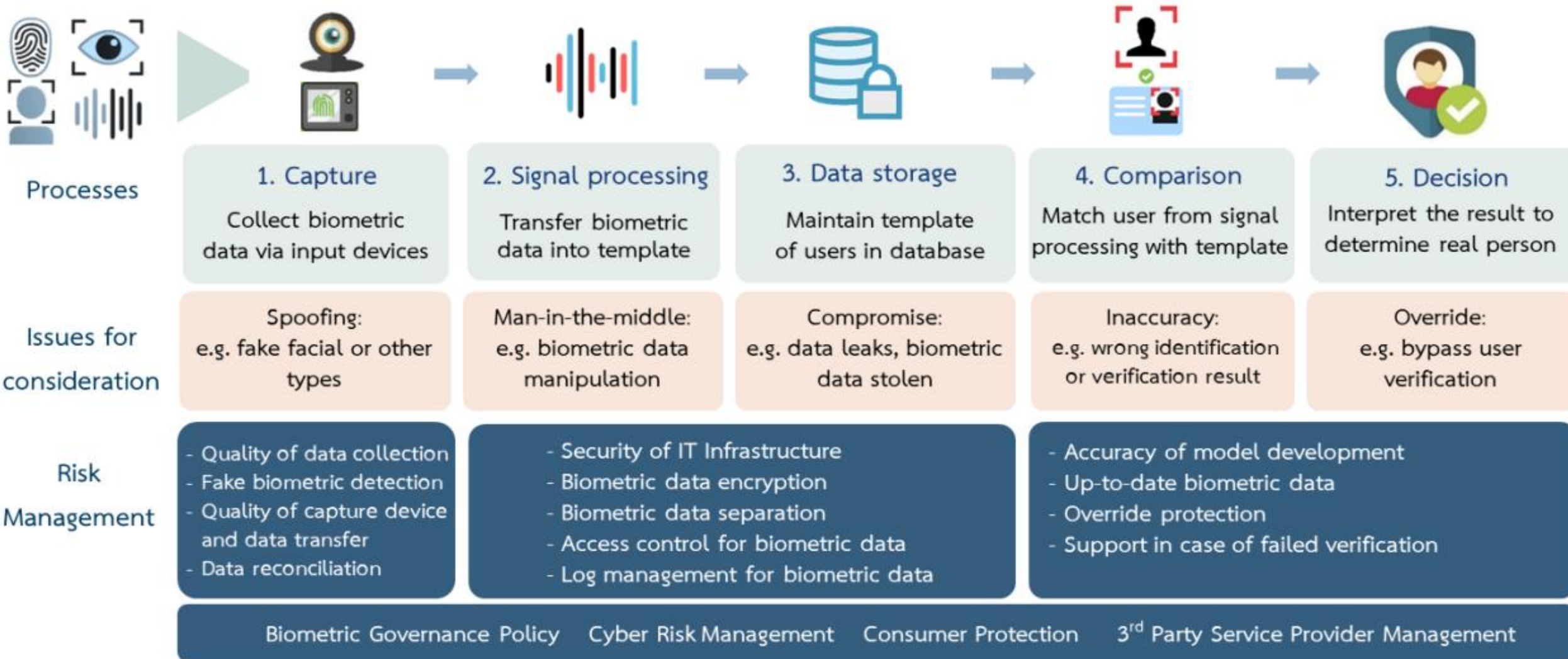
## Biometric Regulatory Landscape and NDID Requirements





# BOT Biometric Technology

## Overview of the Biometric Risk Management Framework



# BOT Summary of Checklist for Biometric Technology Adoption in Financial Services

1. ด้านการกำกับดูแลการใช้เทคโนโลยีชีวมิติ (Governance)	2. ด้านการรักษาความมั่นคงปลอดภัยของข้อมูลชีวมิติ (Confidentiality)	3. ด้านความน่าเชื่อถือของเทคโนโลยีชีวมิติ (Integrity)	4. ด้านความพร้อมใช้ของเทคโนโลยีชีวมิติ (Availability)
G1: การกำกับดูแลการนำเทคโนโลยีชีวมิติมาใช้	C1: แนวทางการดูแลอุปกรณ์ที่ใช้รวบรวมข้อมูลชีวมิติ (Endpoint)	I1: กระบวนการได้มาซึ่งข้อมูลชีวมิติ	A1: แนวทางรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP)
G2: การกำหนดนโยบายสำหรับการกำกับดูแลข้อมูลชีวมิติ	C2: ระบบประมวลผลข้อมูลชีวมิติ	I2: กระบวนการพัฒนาแบบจำลอง	A2: Disaster recovery plan (DRP)
G3: แนวทางในการกำกับดูแลผู้ให้บริการภายนอก	C3: ระบบ IT Infrastructure ที่รองรับการประมวลผลข้อมูลชีวมิติ	I3: ความแม่นยำของแบบจำลอง	A3: มีการทดสอบประสิทธิภาพระบบ IT
G4: แนวทางการดูแลและคุ้มครองข้อมูลของผู้ใช้บริการ	C4: การจัดเก็บข้อมูลชีวมิติ	I4: กระบวนการป้องกันการปลอมแปลงชีวมิติ	
	C5: การรับส่งข้อมูลชีวมิติ		
	C6: กระบวนการควบคุมการเข้าถึงข้อมูลชีวมิติ		
	C7: การบริหารจัดการช่องโหว่ (Vulnerability Management)		
	C8: การจัดเก็บบันทึกเหตุการณ์ (Log) ที่เกี่ยวข้องกับข้อมูลชีวมิติ		

# BOT Summary of Guideline Principles for Biometric Technology Adoption in Financial Services

## 2563 (2020) VERSION

ผู้ให้บริการทางการเงินที่มีความประสงค์จะประยุกต์ใช้เทคโนโลยีชีวมิติประเภทเปรียบเทียบ ภาพใบหน้าของผู้ใช้บริการกับแหล่งข้อมูลที่เชื่อถือได้ (trusted source) ในกระบวนการรู้จักตัวตนลูกค้า ต้องทดสอบการใช้เทคโนโลยีดังกล่าวภายใต้ regulatory sandbox ของ ธปท. โดยต้องปฏิบัติตามเงื่อนไขการทดสอบที่กำหนดโดยครบบถ้วนและได้รับอนุญาตจาก ธปท. ก่อนให้บริการในวงกว้าง

กำหนดให้มีกลไกการกำกับดูแลการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงินที่ชัดเจน เพื่อให้มั่นใจว่ามีการคำนึงถึงการจัดการความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีชีวมิติ ทั้งนี้ อาจใช้โครงสร้างการกำกับดูแลที่มีอยู่ในปัจจุบันหรือที่จัดตั้งขึ้นใหม่เป็นการเฉพาะ โดยโครงสร้างการกำกับดูแลดังกล่าวต้องครอบคลุมการดำเนินงานด้านต่าง ๆ ที่สำคัญ เช่น การวิเคราะห์ความเสี่ยงของเทคโนโลยีชีวมิติ ผลลัพธ์ที่มีการนำเทคโนโลยีชีวมิติมาใช้ และผู้ให้บริการเทคโนโลยีที่เกี่ยวข้อง การกำหนดมาตรการบริหารจัดการความเสี่ยง มาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล และการปฏิบัติตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information technology risk) และแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต้นที่จำเป็น (Cyber hygiene)

ประเมินการนำเทคโนโลยีชีวมิติมาให้บริการอย่างรอบด้านก่อนนำมาใช้ในการให้บริการ ทั้งการประเมินประโยชน์ ความเหมาะสมกับรูปแบบการให้บริการ ผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ความเสี่ยงของเทคโนโลยีชีวมิติ และแนวทางการจัดการความเสี่ยงด้านต่าง ๆ ที่สำคัญ ได้แก่ ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านชื่อเสียง ความเสี่ยงด้านกฎหมายและการปฏิบัติตามหลักเกณฑ์การกำกับดูแลที่เกี่ยวข้อง

## 2567 (2023) VERSION

ผู้ให้บริการทางการเงินที่มีความประสงค์จะประยุกต์ใช้เทคโนโลยีชีวมิติประเภทเปรียบเทียบ ภาพใบหน้าของผู้ใช้บริการ (Facial Recognition) ในกระบวนการพิสูจน์ตัวตนลูกค้าต้องปฏิบัติตาม หลักเกณฑ์ของ ธปท. ที่เกี่ยวข้อง ได้แก่ **หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC)** สถาบันการเงิน **หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)** ของสถาบันการเงิน และ**หลักเกณฑ์การกำกับดูแลความเสี่ยงด้าน เทคโนโลยีสารสนเทศ (Information Technology Risk) ตามกฎหมายว่าด้วยระบบการชำระเงิน**

กำหนดให้มีกลไกการกำกับดูแลการนำเทคโนโลยีชีวมิติมาใช้ในการให้บริการทางการเงินที่ชัดเจน เพื่อให้มั่นใจว่ามีการคำนึงถึงการจัดการความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีชีวมิติ ทั้งนี้ อาจใช้โครงสร้างการกำกับดูแลที่มีอยู่ในปัจจุบันหรือที่จัดตั้งขึ้นใหม่เป็นการเฉพาะ **โดยควรมีผู้เชี่ยวชาญด้านเทคโนโลยีและด้านความเสี่ยงร่วมอยู่ในโครงสร้างการกำกับดูแล** ทั้งนี้ โครงสร้างการกำกับดูแลดังกล่าวต้องครอบคลุมการดำเนินงานด้านต่าง ๆ ที่สำคัญ เช่น การวิเคราะห์ความเสี่ยงของเทคโนโลยีชีวมิติ ผลลัพธ์ที่มีการนำเทคโนโลยีชีวมิติมาใช้ และผู้ให้บริการเทคโนโลยีที่เกี่ยวข้อง การกำหนดมาตรการบริหารจัดการความเสี่ยง มาตรการรักษาความปลอดภัย ข้อมูลส่วนบุคคล และการปฏิบัติตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ประเมินการนำเทคโนโลยีชีวมิติมาให้บริการอย่างรอบด้านก่อนนำมาใช้ในการให้บริการ ทั้งการประเมินประโยชน์ ความเหมาะสมกับรูปแบบการให้บริการ ผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ความเสี่ยงของเทคโนโลยีชีวมิติ และแนวทางการจัดการความเสี่ยงด้านต่าง ๆ ที่สำคัญ ได้แก่ ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านชื่อเสียง ความเสี่ยงด้านกฎหมายและการปฏิบัติตามหลักเกณฑ์การกำกับดูแลที่เกี่ยวข้อง **รวมถึงความเสี่ยงด้านการคุ้มครองผู้ให้บริการทางการเงิน**

# BOT Summary of Guideline Principles for Biometric Technology Adoption in Financial Services

## 2563 (2020) VERSION

ค่าความแม่นยำในการเปรียบเทียบอัตลักษณ์อ้างอิงตามกระบวนการทดสอบมาตรฐานสากล เช่น การพิสูจน์ตัวตนด้วยภาพใบหน้าเทียบกับแหล่งข้อมูลที่เชื่อถือได้ ควรมีค่าอัตราส่วนการยอมรับที่ผิดพลาด (False Acceptance Ratio, FAR) ไม่เกิน 0.1% ตามมาตรฐาน NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management และค่าอัตราส่วนการปฏิเสธที่ผิดพลาด (False Reject Ratio, FRR) ไม่เกิน 3% อ้างอิงตามมาตรฐาน FIDO Biometric Requirements ซึ่งกำหนดกระบวนการ วิธี และระดับความแม่นยำขั้นต่ำในการยืนยันตัวตนด้วยเทคโนโลยีชีวมิติ

ในการทดสอบเทคโนโลยีชีวมิติเพื่อการพิสูจน์และยืนยันตัวตนลูกค้าสำหรับการเปิดบัญชีเงินฝากและเงินอิเล็กทรอนิกส์ ภายใต้กรอบ Regulatory sandbox ของ ธปท. มีการกำหนดจำนวนกลุ่มตัวอย่างทดสอบขั้นต่ำอย่างน้อย 2,000 คน ขึ้นไป

กำหนดให้มีการตรวจสอบกระบวนการรักษาความปลอดภัยข้อมูลชีวมิติของผู้ใช้บริการอย่างสม่ำเสมอ โดยผู้ตรวจสอบภายใน (Internal auditor) หรือผู้ตรวจสอบภายนอก (External auditor) ซึ่งครอบคลุมกรณีที่ใช้บริการจากผู้ให้บริการภายนอก

ความละเอียดของภาพไม่น้อยกว่า 1280 x 720 pixels หรือ 1080 x 1080 pixels

## 2567 (2023) VERSION

ค่าความแม่นยำในการเปรียบเทียบอัตลักษณ์อ้างอิงตามกระบวนการทดสอบมาตรฐานสากล เช่น การพิสูจน์ตัวตนด้วยภาพใบหน้าเทียบกับแหล่งข้อมูลที่เชื่อถือได้ ควรมีค่าอัตราส่วนการยอมรับที่ผิดพลาด (False Acceptance Ratio, FAR) ไม่เกิน 0.1% ตามมาตรฐาน NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management และค่าอัตราส่วนการปฏิเสธที่ผิดพลาด (False Reject Ratio, FRR) ไม่เกิน 3% อ้างอิงตามมาตรฐาน FIDO Biometric Requirements ซึ่งกำหนดกระบวนการ วิธี และระดับความแม่นยำ ขั้นต่ำในการยืนยันตัวตนด้วยเทคโนโลยีชีวมิติ ทั้งนี้ ควรพิจารณาถึงประสิทธิภาพของ Algorithm ของผู้ให้บริการเทคโนโลยีภายใต้การทดสอบของ NIST FRVT 1:1 Verification ควบคู่กัน เช่น มีลำดับค่า False non-match Rate (FNMR) อยู่ภายในผลลัพธ์ 50 ลำดับแรก เป็นต้น

ในการทดสอบเทคโนโลยีชีวมิติเพื่อการพิสูจน์และยืนยันตัวตนลูกค้าสำหรับการเปิดบัญชีเงินฝากและเงินอิเล็กทรอนิกส์ ควรมีการกำหนดจำนวนกลุ่มตัวอย่างทดสอบขั้นต่ำอย่างน้อย 2,000 คน ขึ้นไป ทั้งนี้ ผู้ให้บริการเทคโนโลยีชีวมิติที่ผ่านการประเมินความแม่นยำเทียบกับมาตรฐานสากล โดยองค์กรกลางหรือผู้เชี่ยวชาญที่มีความน่าเชื่อถือ และผลการประเมินอยู่ในระดับที่ ธปท. กำหนด สามารถกำหนดจำนวนกลุ่มตัวอย่างทดสอบขั้นต่ำอย่างน้อย 1,000 คน ขึ้นไปได้

กำหนดให้มีการตรวจสอบกระบวนการรักษาความปลอดภัยข้อมูลชีวมิติของผู้ใช้บริการอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง โดยผู้ตรวจสอบภายใน (Internal auditor) หรือผู้ตรวจสอบภายนอก (External auditor) ซึ่งครอบคลุมกรณีที่ใช้บริการจากผู้ให้บริการภายนอก

ความละเอียดของภาพไม่น้อยกว่า 1280 x 720 pixels หรือ 1080 x 1080 pixels ทั้งนี้ อาจปรับเปลี่ยนขนาดความกว้างและความสูงของภาพให้สอดคล้องกับพัฒนาการของเทคโนโลยีได้ หากยังคงสามารถรักษาระดับความแม่นยำได้ตามเกณฑ์ที่กำหนด

# Significant update on NDID MQA Rev. 2.0. requirements

Topic	Subset (Old version)	Subset (Latest version)
Information Security Governance	Information Security Policy Organization of Information Security	Information Security Policy Organization of Information Contact with Authorities
Asset Management	Asset Management	Asset Management Information Transfer
Access Control and User Management	Access Control	Access Control Human Resource Security Remote Working User End Point Devices
Cryptography and Data Protection	Cryptography Data Protection and Privacy Control	Cryptography Protection of Record Personally Identifiable Information (PII) Data Management
Physical and Environmental Security	Physical and Environmental Security	Physical and Environmental Security
Operational Security	Operation Security Malware Defenses Maintenance, Monitoring and Analysis of Audit Logs Continuous Vulnerability Management	Managing Information Security in ICT Information Security for Use of Cloud Services Malware Defense and Protection Management of Technical Vulnerabilities Logging and Monitoring Installation of Software on Operational Systems

# Significant update on NDID MQA Rev. 2.0. requirements

Topic	Subset (Old version)	Subset (Latest version)
Network and System Security	Boundary Defense	Network Securing System Acquisition and Development
Incident Response and Management	Incident Response and Management	Incident Management
Business Continuity and Compliance	Information Security Aspects of Business Continuity Management	Business Continuity Compliance
	System Acquisition, Development and Maintenance	Change Management
Supplier and Third-Party Management	Supplier Relationships	Legal
Audit and Monitoring	Maintenance, Monitoring and Analysis of Audit Logs	Audit
Security Awareness and Training	Security Awareness and Training Program	Security Awareness and Training Program

# 03

## Biometric Risks and International Standards Safeguards



# BOT Summary of Guideline Principles for Biometric Technology Adoption in Financial Services

## Principles

## Financial Service Providers Obligations and Intended Outcomes

**Principle 1:**  
**Policy framework and governance**

Establish a biometric policy framework, biometric life-cycle data management and governance processes covering **technology risk assessment, vendor risk, risk mitigation plans** including **PDPA, IT risk management guideline, and cyber hygiene** to oversee a robust, efficient and secure biometric technology adoption.

**Principle 2:**  
**Collecting biometric data**

Establish a clear communication message to customers for consent on the purpose and safeguards of biometric data collection. A reliable biometric data collection processes, with robust biometric data quality and integrity for identification, verification, authentication, with the capability of detecting biometric and identity impersonation fraud. **\*\*Customers' biometric data must not be retained in biometric capture devices of financial service providers and in the systems of 3rd party service providers.**

**Principle 3:**  
**Processing biometric data**

Adopt international standards (**FIDO, NIST FRVT, ISO 30107 PAD-attack, ISO 19795 Biometric Performance Testing**) to ensure robust processing accuracy for identify verification, biometric facial recognition and liveness detection against identity manipulation fraud and impersonation attempts from deepfakes, biometric spoofing and identification ID card/passport fraud. **\*\*Customers' biometric data must not be retained in biometric capture devices of financial service providers and in the systems of 3rd party service providers.**

**Principle 4:**  
**Protecting customer's biometric data**

Establish biometric data storage, in secure manner and aligned with international standards (**NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management, PDPA, Data Leakage Controls, Cybersecurity vulnerability assessment and Penetration test**) to ensure that customers' information and biometric data are safely protected.

**Principle 5:**  
**Consumer protection**

Establish a clear communication message to customers for consent on the purpose and safeguards of biometric data collection, biometric life-cycle data management and destruction, consumer protection and PDPA processes to provide safe and sound services.

**Principle 6:**  
**Operational risk management**

Establish **business continuity plans** to manage significant operational risks, **fraudulent transaction monitoring** and **third-party service management (BOT Notification No. Sor Gor Chor. 5/2566)** to ensure the safety and trust of customers.

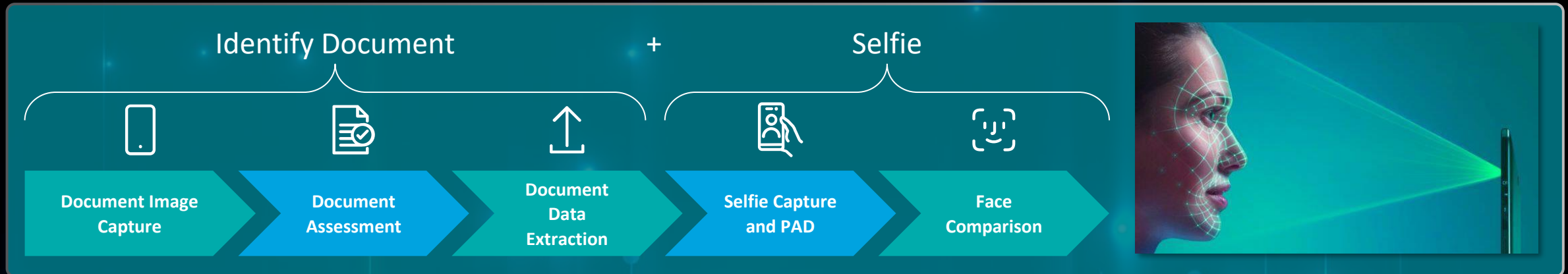


# Identity Verification Proofing Process

Identity verification is the combination of activities during a remote interaction that brings a real-world identity claim within organizational risk tolerances

## Key Steps in the Identity Validation Process

A layered approach that combines government-issued ID scan, a selfie and 3D liveness detection.



### Identity Document Verification

- Prompt the user to take an image of a valid government-issued ID document (driver's license, passport or ID card).
- Data is extracted from the document by optical character recognition (OCR).
- Validate the authenticity of a government-issued photo identity document that is either validated by an algorithm or human means for authenticity.

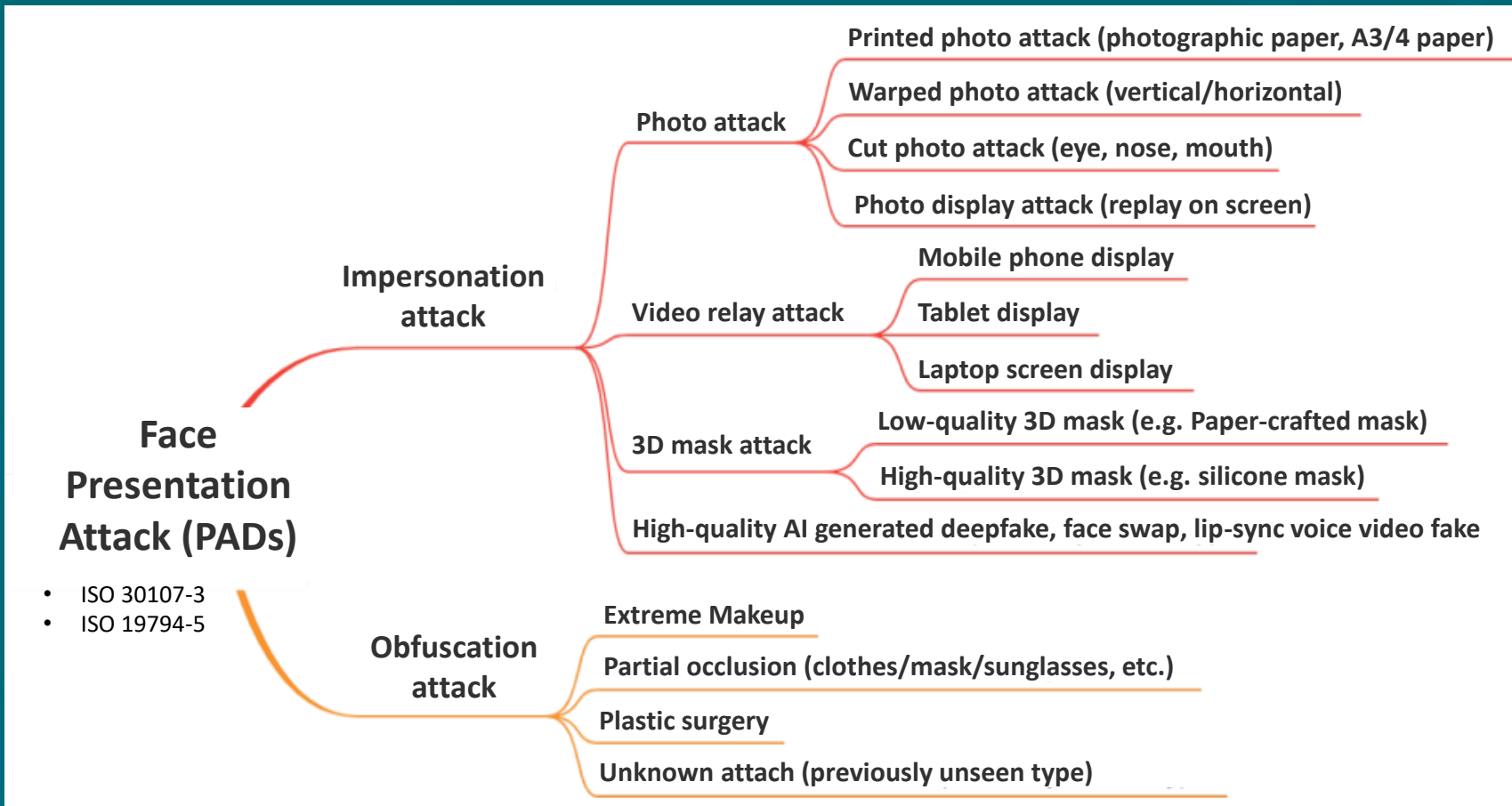
### Biometric Facial Verification

- Validate whether the user is the genuine owner of the identity document by prompting the user to take an image or short video of their face which is assessed for liveness (formally called PAD).
- Validate biometrically and compares it with the photo on the document and/or the biometric original reference data and photo in the database to verify and unlock the user's digital identity in seconds.

# Common Liveness Spoofs

Known vulnerabilities in liveness detection methods which are susceptible to liveness spoofing.

Cyber-criminals are using spoofing attacks and deepfakes biometric and voice manipulation technology to outsmart biometric systems. Examples of the attacks are shown below.



voice content.

# High Fraud Risk Indicators Testing & Evaluation

Comprehensive testing needs to be performed to validate the fraud controls. Below outlines some examples of the high fraud risk indicators on fake ID card/passport and tampering.

Indictors

What are the triggers?

What needs to be tested?

## Best Practice

### A Robust eKYC Identity and Biometric Verification

Technology will Always Use

“Live-Capture” Mode on the Mobile Devices

to Capture the Biometric Images and Videos

For Identity Verification Processing

Biometric Facial  
Recognition Robustness

Document Verification

# Best Practice | System Test and Attack Analysis: Approach

## Factors: Zero Information Attack, False Match Rate (FMR) and Presentation Attack Detection (PAD)

Assumptions & Approach	False Match Rate (FMR)	Presentation Attack Detection (PAD)	FIDO Level	PAD Intensity	Artifacts
<ul style="list-style-type: none"> <li>Isolate the aspects of biometric technologies that can be quantified</li> <li>Assume a baseline of “cyber hygiene”</li> <li>Assume FMR and PADER are independent of one another</li> <li>Inherent biometric strength, “Zero information” attacks, i.e., the attacker does not have the PIN or biometric pattern</li> <li>Observation of additional controls (e.g., limiting failed attempts) may be layered on top of the quantified strength to improve the overall security of a system</li> </ul> <p>When authentication limit has been reached:</p> <ul style="list-style-type: none"> <li>Delay 30 seconds before next authentication, and increase delay time exponentially 30 secs, 1 minute, 2 minutes, 4 minutes and 8 minutes.</li> <li>Deny authentication and recommend using other method.</li> </ul> <ul style="list-style-type: none"> <li>Identify the relevant factors for the test framework</li> </ul>	<p><b>Probability of a false match occurring</b></p> <ul style="list-style-type: none"> <li>Proportion of impostor attempt samples falsely declared to match the compared template</li> <li>Empirically determined</li> <li>Combination of inherent discrimination, signal fidelity; sensor performance; processing and matching capabilities</li> </ul> <p>*BOT threshold requirements: False Acceptance Ratio (FAR) &lt; 0.1% False Reject Ratio (FRR) &lt; 3%</p> <ul style="list-style-type: none"> <li>Number of authentication attempts</li> </ul> <p>*ETDA threshold requirements: Failed authentication attempts &lt; 5x for normal case and &lt; 10x for PAD.</p>	<p><b>Probability of a successful presentation attack</b></p> <ul style="list-style-type: none"> <li>Proportion of presentation attacks incorrectly classified as bona fide presentations at the PAD subsystem in a specific scenario</li> <li>Error rates and test level as defined in NIST FRVT, ISO/IEC 30107-3 and FIDO Alliance</li> <li>Biometric Performance Test standards as dictated by ISO 19795</li> <li>NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management,</li> <li>Type of attacks used on Artefact Detection (AD) and Liveness Detection (LD)</li> <li>Types of tests: verifying vendor claims, and/or different level of sophisticated attacks</li> </ul>	<p><b>Level A</b></p> <p><b>Level B</b></p> <p><b>Level C</b></p>	<p>Time: Short Expertise: Anyone Equipment: Readily available</p> <p>Time: &gt; 3 days Expertise: Moderate skill Equipment: Available but requires planning</p> <p>Time: &gt; 10 days Expertise: Extensive skill Equipment: Specialized and not readily available</p> <p>Source of biometric characteristic: Easy to obtain</p> <p>Source of biometric characteristic: Difficult to obtain</p> <p>Source of biometric characteristic: More difficult to obtain</p>	<p>Paper printout of face image, mobile phone display of face photo</p> <p>Photo from social media</p> <p>Paper masks, video display of face (with movement and blinking)</p> <p>Video of subject, high quality photo</p> <p>Silicon masks, theatrical masks, Deepfake, face swap and AI generated face image</p> <p>3D face information from subject</p>

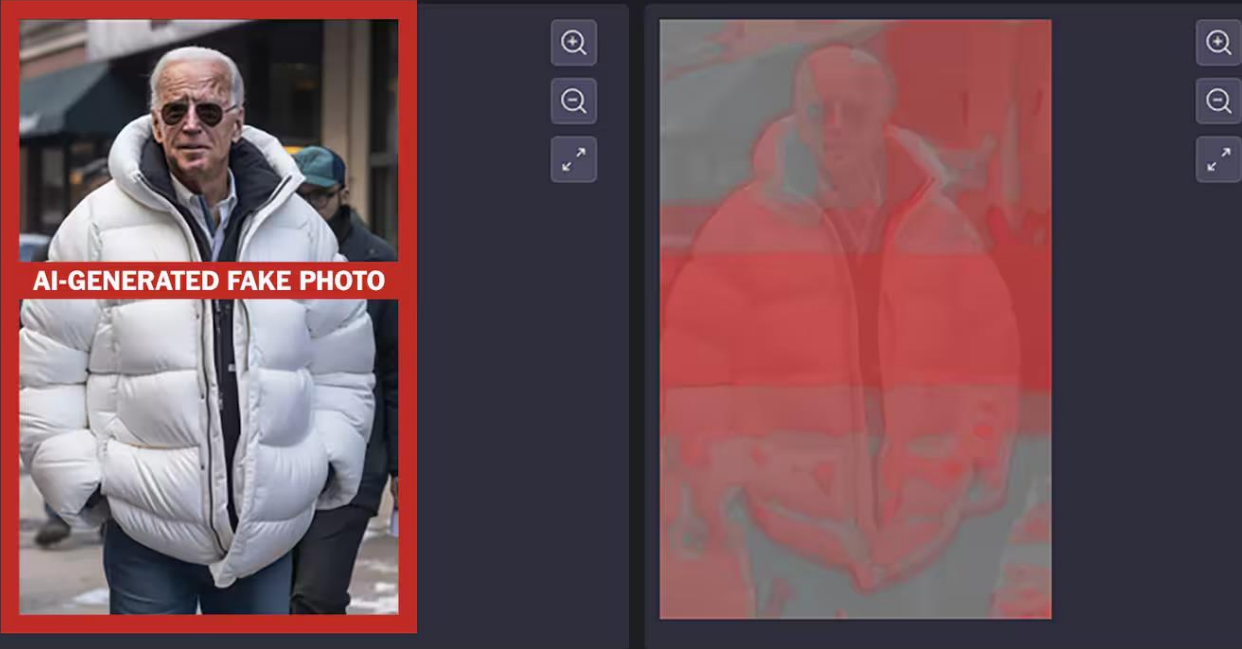
# Keeping Up With Compliance With AI | Deepfake Detection Tool

With the growing number of deepfakes, Deepfake detection software is becoming increasingly popular to protect against the harmful effects of fake videos and audios.

**fake\_biden\_1.png**

73%

Duration: 1 Image    Upload date: 03/07/2024    Modality: Image    Falsehood probability: Likely Fake ⓘ



**AI-GENERATED FAKE PHOTO**

Source: DeepMedia

Media Name: Image - Gabe    Source: Reality Defender

Media Details ⓘ

TYPE: Image    FORMAT: jpg

SIZE: 344.49 KB    UPLOADED DATE: Thu Mar 14 2024

Helpful Tips

- Read the model description to better understand what each model is built to detect.
- Higher resolution and uncompressed media files will generally provide more accurate results.
- Our models will potentially return no results if faces in the media file provided cannot be properly detected. Some reasons for this include: no faces, faces that are too small, and faces that are posed at extreme angles.

**MANIPULATION DETECTED**




Image Detector - Ensemble	99.00%	Likely Manipulated	Combines the fakeness scores from all four Image Detector models into a single, more accurate fakeness score	Explanability ⓘ
Image Detector - Visual Noise Analysis	77.75%	Likely Manipulated	Detects fake images by analyzing the texture of the visual noise	Explanability ⓘ
Image Detector - Faceswaps	1.00%	Unable to detect manipulation	Detects faces manipulated using faceswap methods	Explanability ⓘ
Image Detector - Diffusion	1.00%	Unable to detect manipulation	Detects fake images created using diffusion methods	Explanability ⓘ
Image Detector - GANs	99.00%	Likely Manipulated	Detects images of faces that are generated or manipulated using GANs	Explanability ⓘ

# Summary Recap

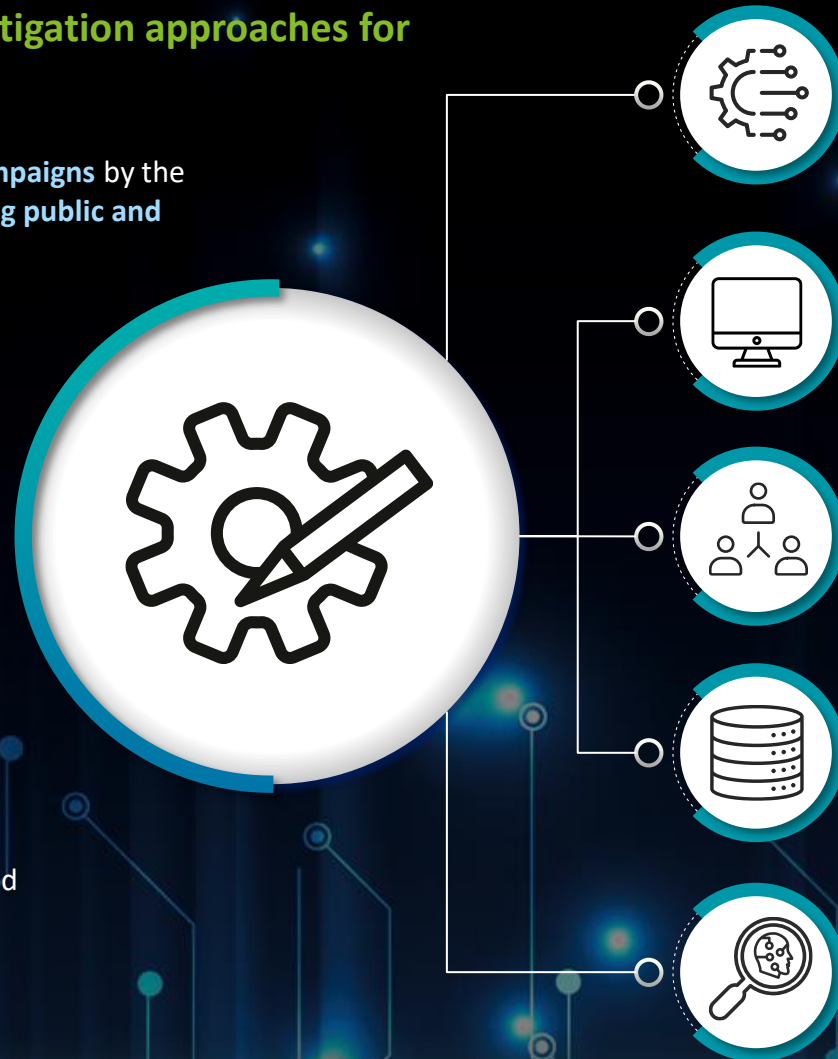


# Best Practice for Biometric, Identity Fraud and Deepfake Risk Mitigation Strategies

Requires tripartite efforts from the Government, Banks and Public (Customers)

**On the right are some of the risk mitigation approaches for organisations against deepfakes.**

- Deepfake, Phishing and Smishing **national campaigns** by the government and banks are effective in **creating public and user awareness** and **vigilance**.
- Bank customers' **biometric data** should be **current** and kept **up to date** within the **24 months** period.
- Storage of **customers' data** and **biometric sensitive PII** should be **segregated** to increase **data protection** and **cyber security robustness**.
- Mitigating biometric, identity fraud and deepfake attacks demands a **multi-layered strategy** that incorporates **technological innovations**, **proactive detection** methods, and **robust authentication mechanisms**.
- Implementing **AI-driven detection systems** and constantly **staying updated with evolving algorithms** (to recognise patterns unique to deepfakes) forms a **critical layer in combating** these **threats**.



**Emerging technologies**  
Adapting and enhancing the detection technology with emerging technologies, such as the following:

- Watermarking audio files
- Photo plethysmography (PPG)

**Continuous monitoring**  
Organisations should continuously monitor and authenticate the incoming voice/video prints used for biometric authentication.

**User awareness**  
Raising awareness about deepfake attacks and its associated risks will help in making customers more vigilant and better equipped.

**Analysis of stored audio/facial data**  
Continuous refinement and improvement of biometric algorithms is essential to enhance detection accuracy.

**Behaviour analysis**  
Examining patterns in a user's speech/video, such as tone, lip-sync, etc., identify anomalies that may indicate a deepfake attempt.

# 04

## How Deloitte Can Help





# How We Can Help

We have the technology, process understanding, a proven approach and experience team in conducting risk management assessment on the Identity Verification, Biometric Facial Recognition, Liveness Detection and Document Validation.



## Research and Point of View in KYC/CDD and AML

Our KYC/AML Best Practice Framework contains best practice process & sub-process models, performance benchmarks, and technology enablers.



## We have done similar eKYC projects before

We are leveraging on our experience on similar projects, and a team who understands the eKYC process, biometric and new technologies in the areas of machine learning/artificial intelligence and analytics for eKYC/CDD, identity verification, biometric facial recognition, liveness detection and document validation.



## Understand the APAC Requirements

We understand the eKYC/CDD and biometric regulatory requirements and legislation in Thailand, Singapore, Malaysia, Hong Kong and across Asia Pacific.



## Proven Testing Methods & Accelerators

We have tailored our approach based on our proven review and assessment methodology, and our understanding of similar biometric technologies in the eKYC/AML operations.

# Our Services

Deloitte is at the forefront of defining, researching and transforming the complexity of the IT audit, general and application controls, regulatory compliance and emerging digital risk management today.



## IT Audit, Risk and Control Advisory

IT Audit – General & Specific Controls Review  
(IPO, ITDD, PMI, QAR, etc.)

IT Governance & Security, Risk & Control Assurance

SOX/JSOX IT Control Implementation & Test

Third Party Risk Management & Assurance

Audit Data Analytics



## IT Compliance Review & Member Assessment

Bank of Thailand (BOT)

IT Risk Management, Third Party Risk, API Security, Biometric Processing, Data Governance, Cyber Resilience, etc.

Securities & Exchange Commission (SEC)  
IT Governance, Security, Audit, etc.

Office of Insurance Commission (OIC)  
IT Governance, Security, Audit, etc.

IT Audit – PDPA, NCSA  
Assessment – NDID (MQA), PCI-DSS  
SWIFT Customer Security Control Framework

# Let's talk

If you're ready to move from abstraction to action, contact us for a complimentary discussion session.



**Chinkavin Kittanatchai**

Partner

Email: [ckittanatchai@deloitte.com](mailto:ckittanatchai@deloitte.com)

**Nattaseth Tirawattananont**

Assistant Manager

Email: [ntirawattananont@deloitte.com](mailto:ntirawattananont@deloitte.com)

**Joeyvoen Teo**

Senior Manager

Email: [joteo@deloitte.com](mailto:joteo@deloitte.com)



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

#### **About Deloitte Thailand**

In Thailand, services are provided by Deloitte Touche Tohmatsu Jaiyos Co., Ltd. and its subsidiaries and affiliates. This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.