EU AI Act:

Outlining the practical steps to achieving AI compliance in day-to-day financial services operations

Cameron Craig
Deputy General Counsel
Global Head of Data Legal

HSBC

November 2024

AI use in Financial Services

75%

of firms are using AI. **10%** more plan to in the next 3 years

Foundation models (including LLMs) make up **17%** of AI use cases

33%

of AI use cases are from 3rd parties

55%

of AI use cases have some automated decision-making. Only **2%** are fully autonomous

62%

of AI use cases are low materiality vs **16%** high (as rated by firms)

Greatest perceived benefits are in data & analytical insight, AML & combatting fraud, and cybersecurity

Greatest perceived risk is cybersecurity. Growing risks are 3rd party dependencies, model complexity, and embedded models

84%

of firms have a person accountable for AI

34%

of firms have 'complete understanding' of the AI they use, **46%** have a 'partial understanding'

FCA FINANCIAL CONDUCT AUTHORITY

EU AI Act – an outline

European Union sets out a legal framework that aims to regulate the design, development, deployment, and use of AI systems in EU.
The act defines standard classification for the AI systems based on the risk they pose to users.

By the Act's definition, 'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments

EU gives priority to make sure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly.
AI systems should be overseen by people, rather than by automation, to prevent harmful outcomes.

PURPOSE

Promote human-centric and trustworthy AI

Protect health, safety, fundamental rights, democracy and the rule of law

Prevent harmful effects on the environment

Support innovation

ROLES IN THE AI VALUE CHAIN

Provider: An Entity that develops an AI System commercially or part of their service.

Deployer: An Entity using an AI system under its authority

Distributor: An Entity in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market

Importer: An entity located or established in the EU that places on the market an AI system that bears the name or trademark of an entity established outside the EU.

SCOPE

Providers of AI Systems, irrespective of whether those providers are established or located within the Union or in a third country

Deployers of AI systems that have their place of establishment or are located within the Union

Providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union

Importers and distributors of AI systems;

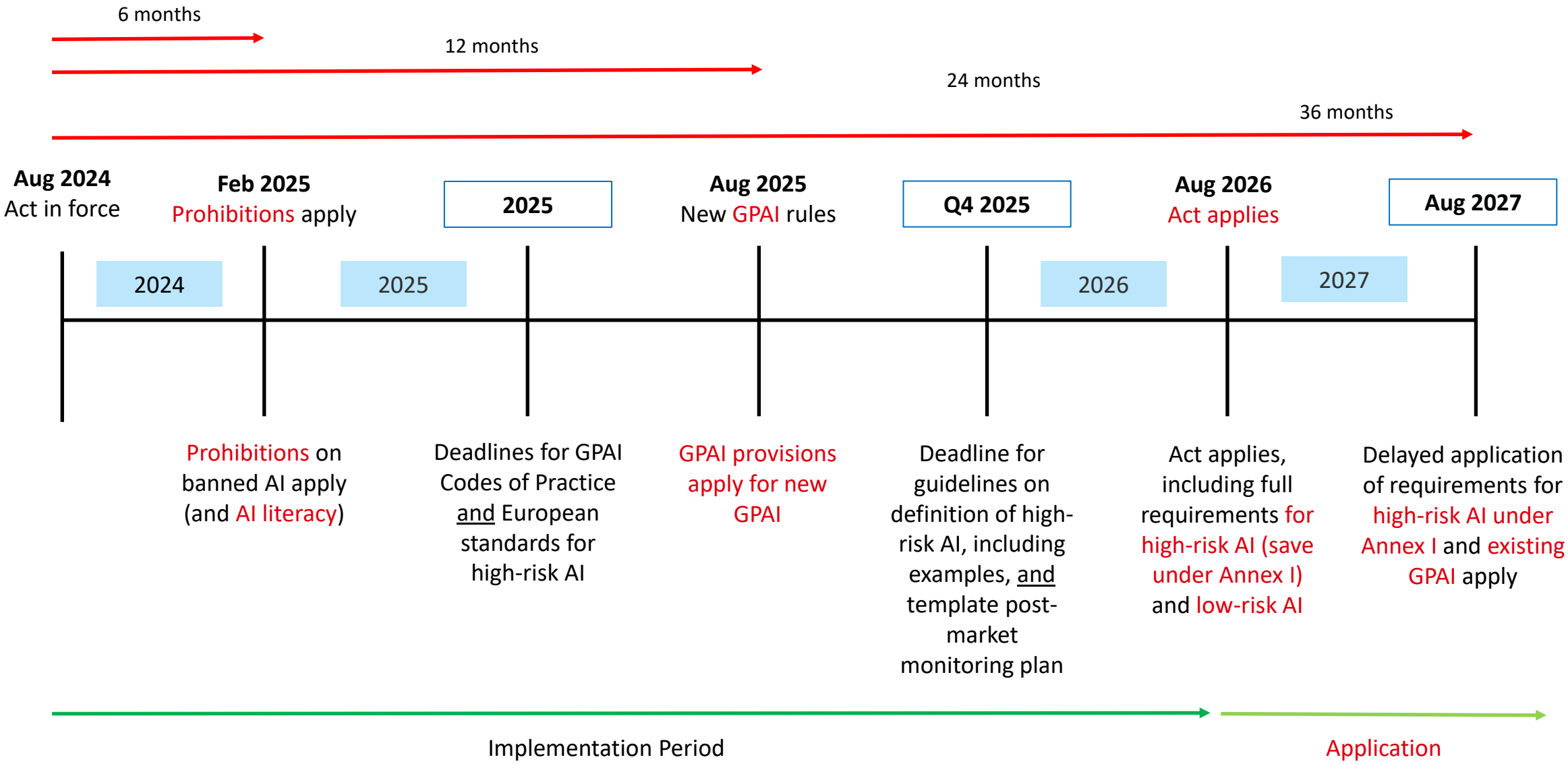
ENFORCEMENT

EU-wide authorities coordinate across member states

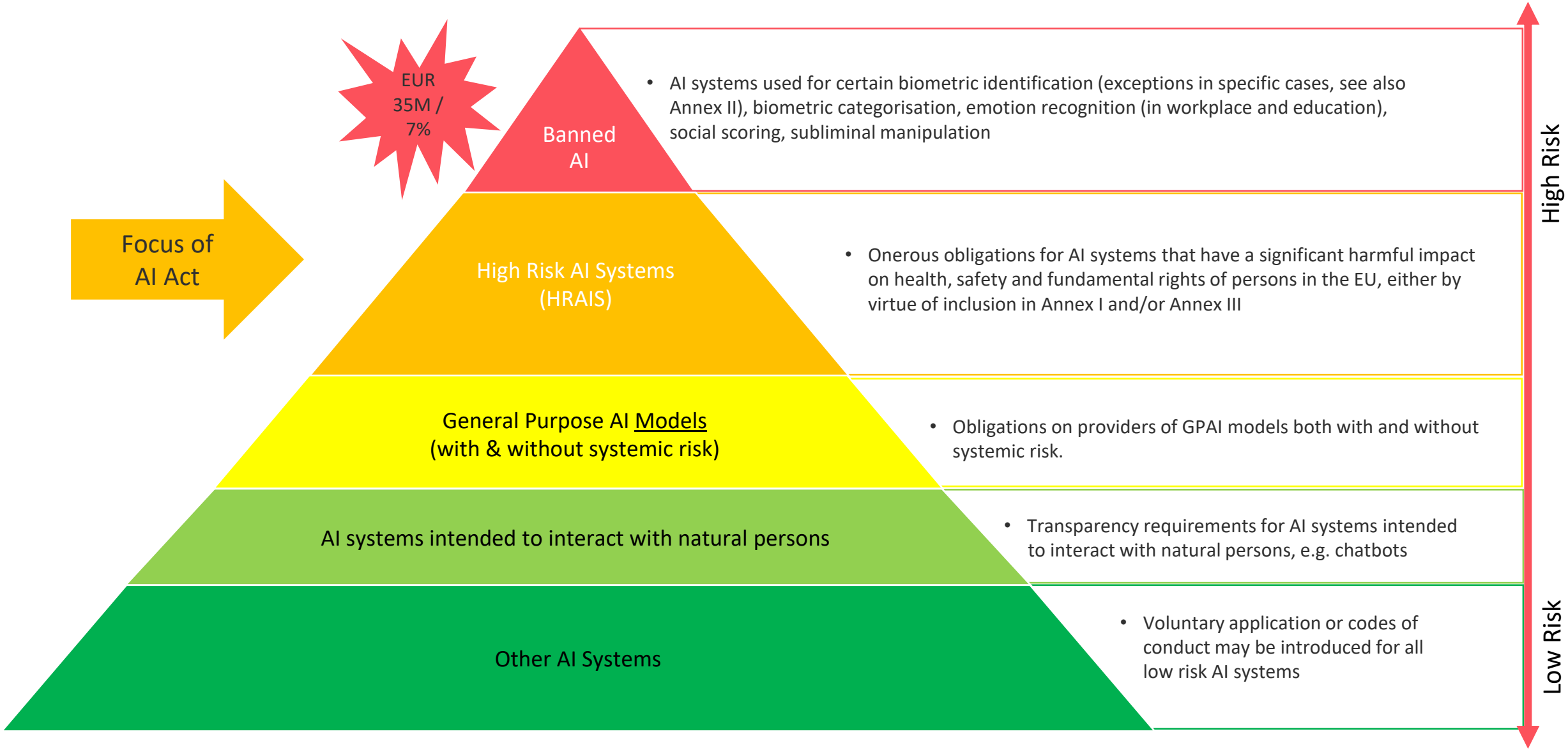
National supervisors enforce compliance, appointing "notified bodies"

Fines up to 35m€
or 7% of global annual turnover for use of prohibited AI systems and up to 15m€ or 3% of g.a.t. for breach of
High-Risk AI system requirements and transparency obligations

EU AI Act – key timings

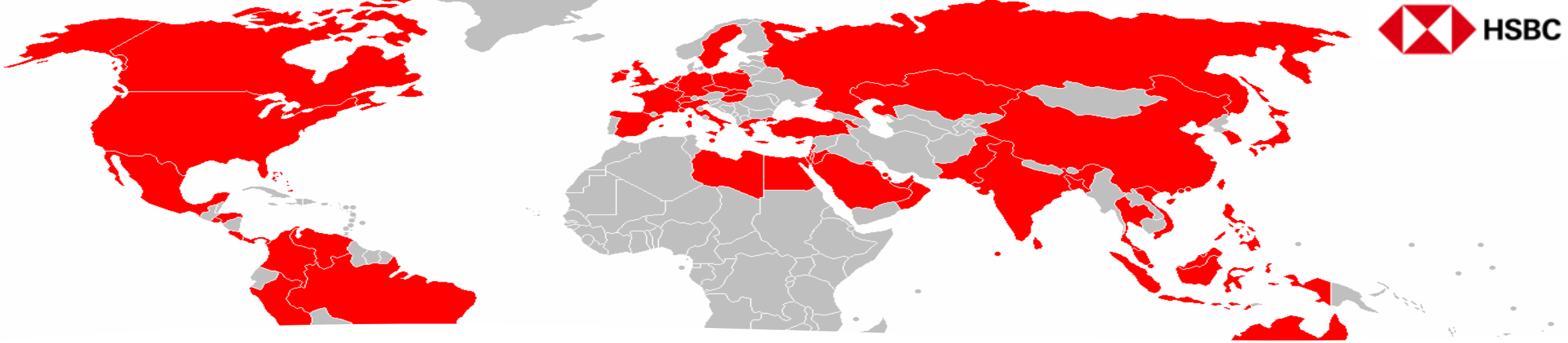


EU AI Act – Risk based approach



The blacklist - Prohibited AI Systems

- Using subliminal, manipulative or deceptive techniques, or to exploit vulnerabilities
- Evaluating or classifying persons based on social behaviour or personality characteristics (social scoring)
- AI to risk assess criminal activity based solely on profiling of personality traits and characteristics
- Creating or expanding facial recognition databases using non-targeted scraping from internet or CCTV
- Inferring emotions in the workplace/education setting (emotion recognition systems)
- Using protected characteristics/attributes to infer or categorise according to sensitive characteristics (biometric categorisation systems)
- Use of ‘real-time’ remote biometric identification in public



HSBC

Practical Compliance Challenges

- Getting the scope right – AI and role definition
- Horizontal risk – allocating accountability across the verticals
- Defining the “delta” to existing processes
- Accountability and identifying dependencies
- Aggregating across different global standards – many to few
- Third party use of AI
- Monitoring ongoing compliance of an autonomous system

AI Governance Framework – outline approach