CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

AI SHARED RESPONSIBILITY MODEL

VERSION 1.0 | AUGUST 2025| TLP CLEAR

CMORG-endorsed capabilities (including good practice guidance, response frameworks and contingency tools) have been developed collectively by industry to support the operational resilience of the UK financial sector. The financial authorities support the development of these capabilities and collective efforts to improve sector resilience. However, their use is voluntary, and they do not constitute regulatory rules or supervisory expectations; as such, they may not necessarily represent formal endorsement by the authorities.

AI SHARED RESPONSIBILITY MODEL

CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

FOREWORD

This Shared Responsibility Model (SRM) provides baseline guidance for understanding Artificial Intelligence (AI) security responsibilities and how these are managed between client firms and AI service providers. Its focus is solely on the security aspects of AI adoption: broader topics such as privacy, ethics, or general model risk are outside its scope.

The SRM primarily addresses security for Foundation Models *(FMs)* delivered as a service. While custom AI models exist, this guidance centres on FM usage. The SRM uses the stablished infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service SaaS structure. Responsibilities are colour-coded (AI service provider, financial services organisation, or shared) for clear visual understanding.

AI services are diverse. While this model is high-level and generally applicable, specific implementations may vary. It is a foundational guide, adaptable to unique AI use cases and deployment scenarios (e.g. on-premises, edge AI). Its purpose is to initiate clear discussions and promote secure adoption of AI in the evolving AI landscape.

OVERVIEW

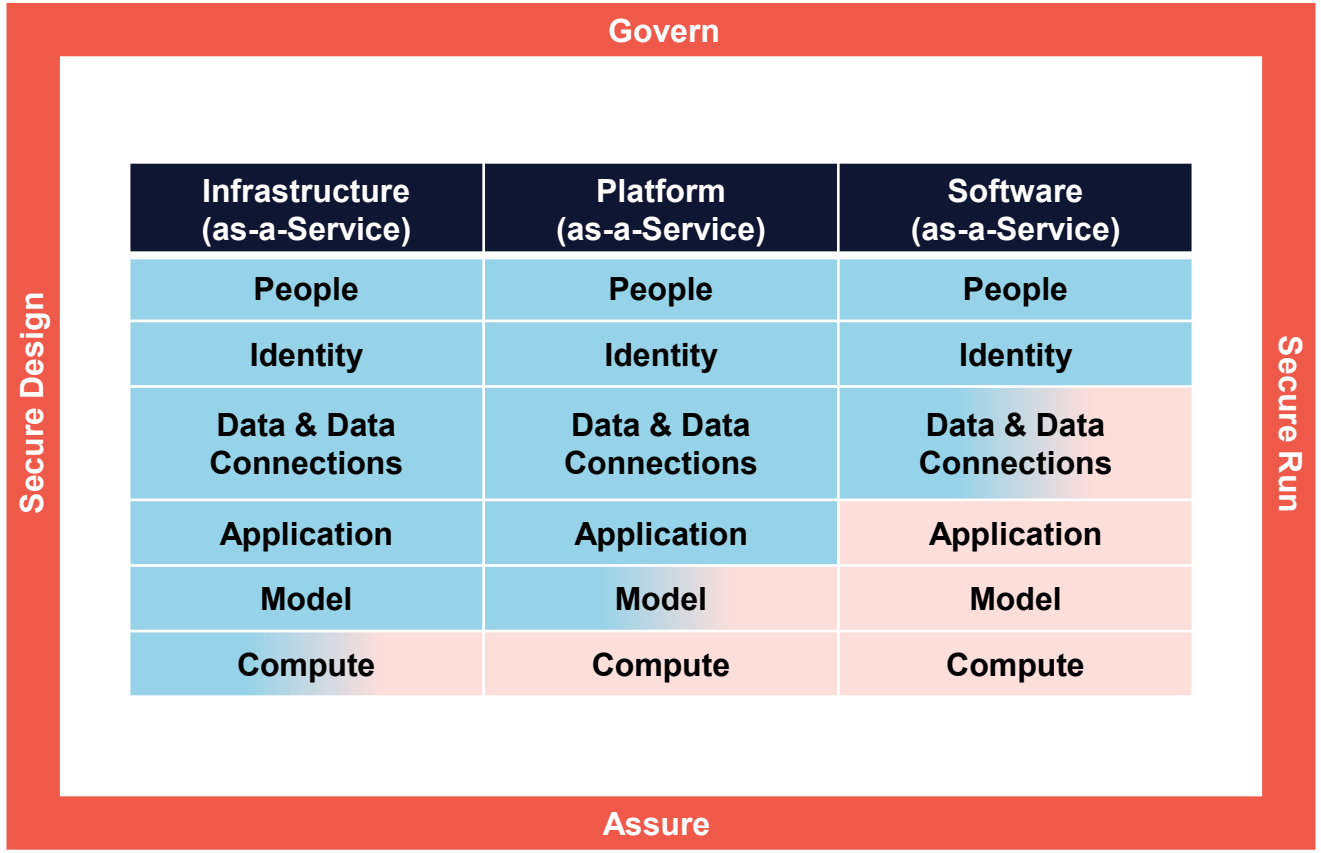
- This initiative has been delivered through CMORG's AI Taskforce, comprising CIO and CISO-level representatives and broad engagement from across the financial services sector, along with close collaboration with major AI service providers to ensure the framework is both practical and representative of needs of all key stakeholders.

OBJECTIVE

- The purpose of the SRM is to establish an approach that provides an agreed baseline structure, endorsed by industry and AI service providers, for managing implementation risks between AI service providers and FS firms. The model aims to minimise the potential for divergences in approach that could lead to operational impacts at the firm or sector level.
- The SRM establishes clear accountability across the model, supporting greater consistency in implementation across the financial sector, while helping firms clarify key objectives during AI adoption. It also builds on existing models, leveraging a range of current AI frameworks to ensure relevance and support alignment.

AI SHARED RESPONSIBILITY MODEL

CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP



Infrastructure (as-a-Service)	Platform (as-a-Service)	Software (as-a-Service)
People	People	People
Identity	Identity	Identity
Data & Data Connections	Data & Data Connections	Data & Data Connections
Application	Application	Application
Model	Model	Model
Compute	Compute	Compute

Legend

AI Service Provider	FS Organisation	Shared

AI SHARED RESPONSIBILITY MODEL

CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

KEY CONTROL GROUPS

1. **People**: Ensuring the competence, training, and appropriate use of AI systems by FS organization personnel.
2. **Identity & Access Management:** Securely manage identities and access control for authorized personnel, models, and systems interacting with AI resources.
3. **Application & (Application) Infrastructure**: Develop, deploy, and operate robust and secure software. Secure the infrastructure supporting the application.
4. **Data & Data Connections:** Ensuring the integrity, security, and lifecycle management of all AI-related data (excluding training data), including input prompts, inference data, and generated outputs. Securing and managing external data sources, plugins, and connections.
5. **Model**: Manage the entire AI model lifecycle, addressing model security and risk. This includes performance validation, version control, ethical considerations, and ongoing monitoring for model drift.
6. **(IT Compute) Infrastructure**: Secure the underlying compute infrastructure supporting AI systems. This includes physical security, network security, operating system hardening, and access controls.
7. **Govern**: Establish and maintain the AI governance framework, encompassing policies, procedures, risk management, compliance, and alignment with organizational strategy.
8. **Secure Design**: Integrate security and privacy into the design and development phases of AI systems. Use Security-by-Design and Privacy-by-Design approaches, ensuring controls are embedded from the outset.
9. **Secure Run:** Ensure secure and reliable operation of AI systems in production. This involves runtime monitoring, incident response procedures, and maintaining system integrity.
10. **Assure**: Assess and validate AI systems through audits, continuous monitoring, penetration testing, and compliance checks. Provide independent verification of security and ethical operation.

AI SHARED RESPONSIBILITY MODEL

CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

DEFINITIONS

SaaS
Software-as-a-Service

AI embedded within software applications to enhance functionality and user experience, often focusing on specific tasks or domains.

PaaS
Platform-as-a-Service

AI development and deployment platforms that provide pre-built tools, libraries, and infrastructure to facilitate the creation of AI-powered applications.

IaaS
Infrastructure-as-a-Service

Infrastructure resources (compute, storage, networking) optimized for AI workloads, allowing for scalable and efficient training and deployment of AI models.