




# Regulating Third-Party Cyber Risk in Financial Services

## Practitioner Perspectives on DORA in the UK and US Regulatory Context

### INTRODUCTION

- Financial institutions increasingly rely on third-party ICT providers, increasing cyber risk
- Incidents affecting third parties can disrupt financial services
- Third-party breaches are costly, and supply chain risk is a top global threat
- The Digital Operational Resilience Act (DORA) strengthens operational resilience in the EU
- Limited research examines practitioner implementation of DORA

### RESEARCH QUESTIONS

-  **Effectiveness**  
Perceived effectiveness of DORA in managing third-party cyber risk
-  **Implementation**  
Challenges faced by practitioners when implementing DORA requirements
-  **Governance**  
Evaluation of governance and control mechanisms for third-party ICT risk

### METHODOLOGY

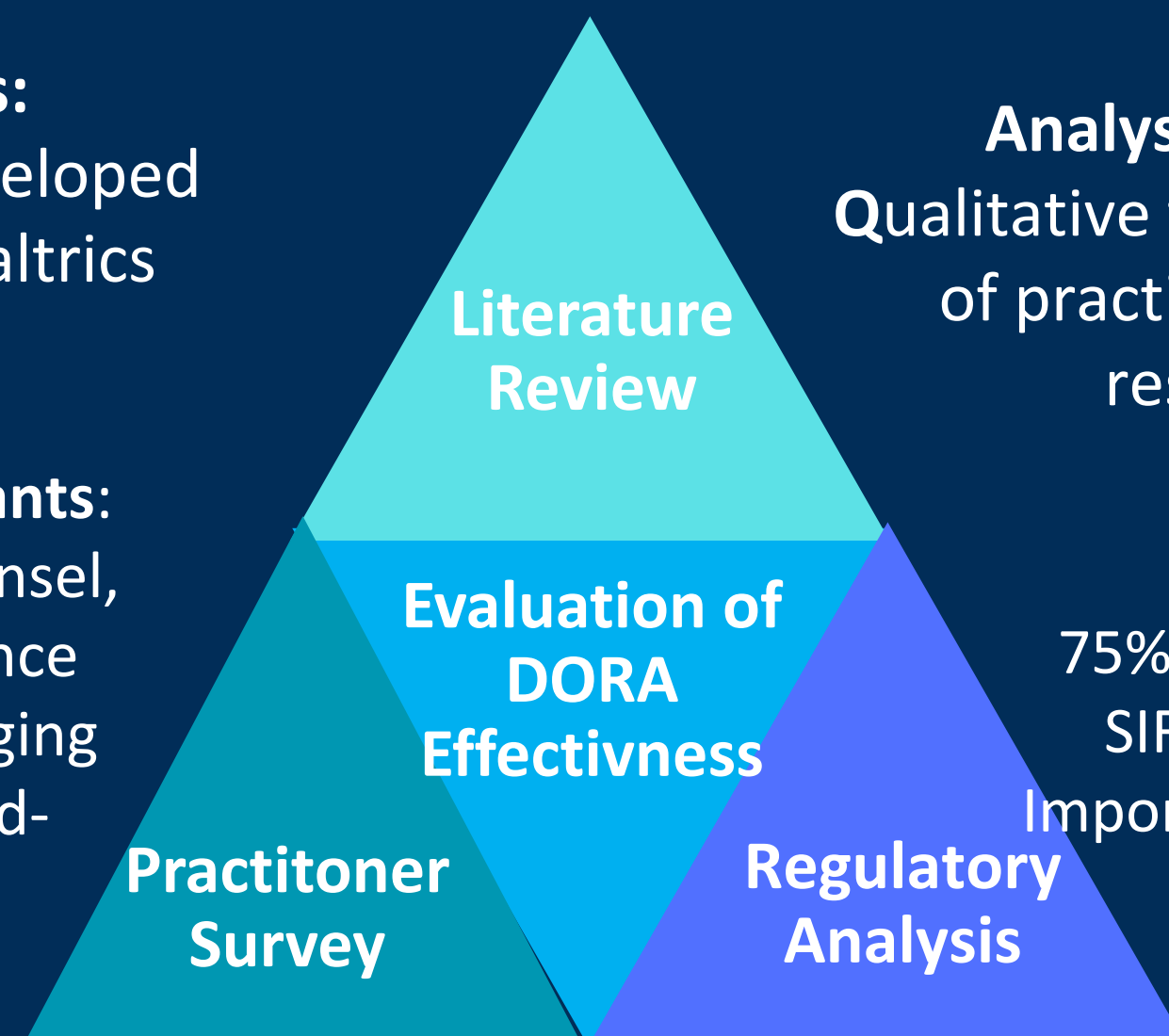
Findings triangulated across practitioner survey, regulatory analysis & literature to enhance validity & reliability

**Tools:**  
Survey developed using Qualtrics

**Analysis Method:**  
Qualitative thematic analysis of practitioner survey responses

**Participants**  
75% of Participants from SIFMU - Systemically Important Financial Market Utility

**Target Participants:**  
Senior legal counsel, Chief Compliance Officers, Managing Director, Third-Party Risk



### LITERATURE REVIEW

- Cyber risk is increasingly driven by third-party and supply chain dependencies
- Limited visibility over subcontracting chains creates systemic risk
- Existing UK/US frameworks are principles-based and flexible, leading to variation in implementation
- DORA introduces a more prescriptive, standardised approach to improve oversight

### KEY FINDINGS

**DORA improves oversight and visibility but introduces operational complexity - an increased burden that may be necessary given the scale of third-party cyber risk.**



Cyber risk increasingly threatens **financial stability**



Supply chain vulnerabilities represent a major source of **cyber risk**



Cloud provider **concentration** may create systemic risk

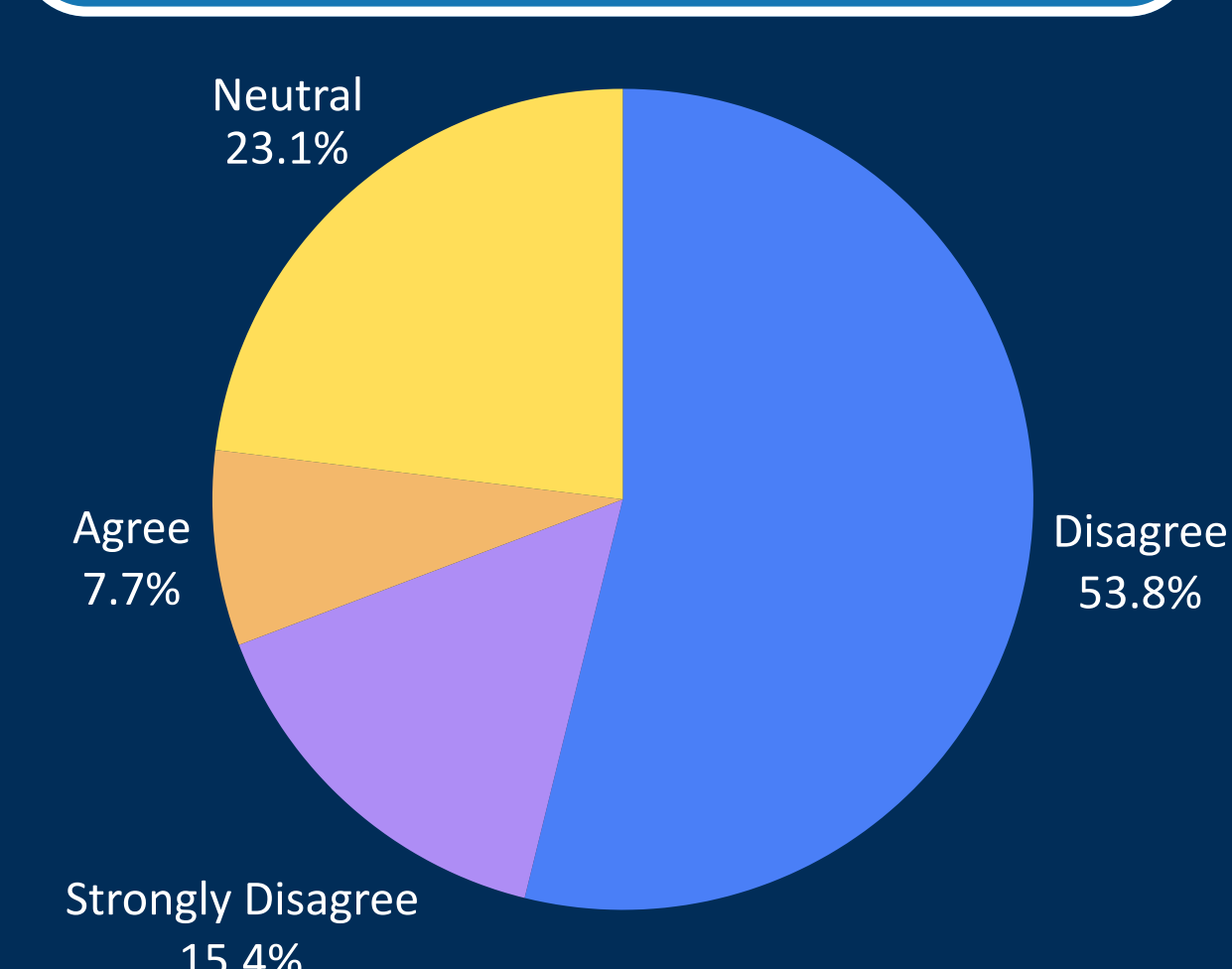
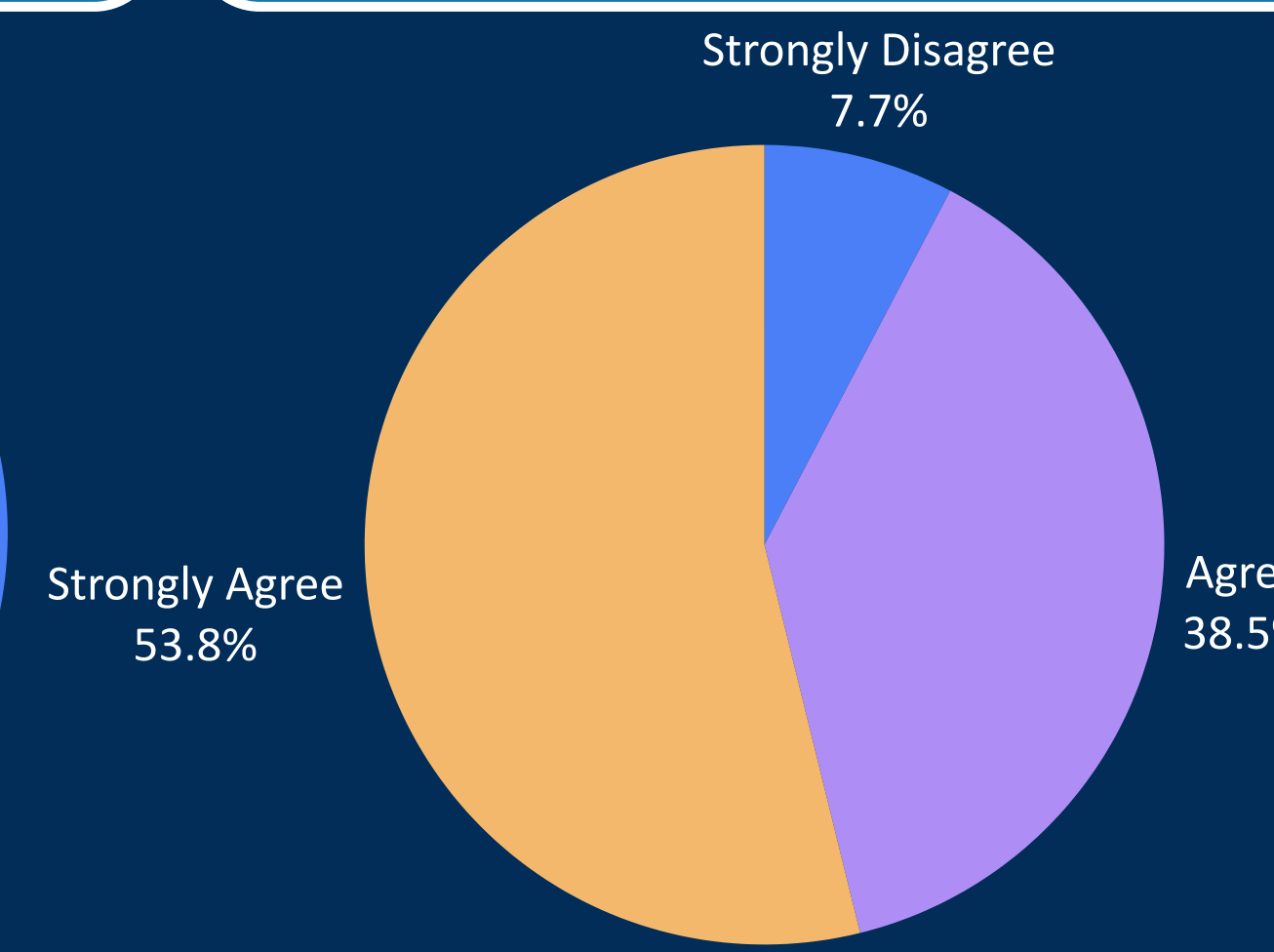
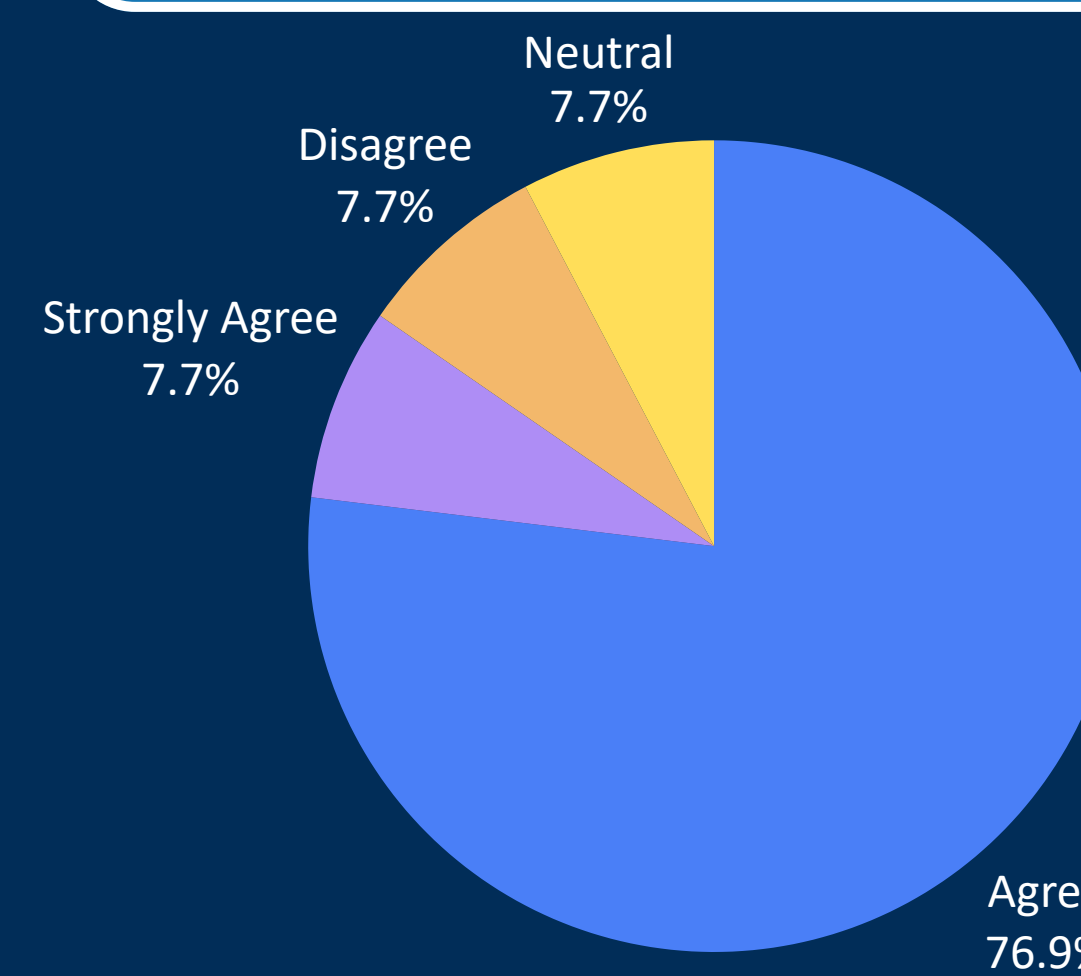


Regulatory frameworks such as **DORA strengthen operational resilience**

**DORA improves oversight**

**Implementation requires significant operational effort**

**DORA is straightforward to implement**



**NEXT:** Analyse practitioner insights, compare EU/UK/US approaches & complete the dissertation



**Student :** Elaine McConnell  
C00315730@setu.ie  
**Supervisor :** Michael Gleeson