Broadridge

Ready for Next

Digital Operational Resiliency Act (“DORA”)
Der Weg zu verbesserter operativer Resilienz

Heidi Dittmar – Managing Director Germany
Baris Yildirim – Sales Director, DACH & CEE

WM Kundenforum
7. November 2024

Agenda

- Introductions & Overview
- DORA Insights
- Readiness Assessments – a possible approach
- Regulation as the opportunity to innovate

Broadridge [NYSE:BR] at-a-Glance

IDC FinTech Rankings 2023
#3 FinTech | Fast Track FinTech

Broadridge, a global fintech leader with $6+ billion in revenue, provides communications, technology, data and analytics.

We help drive business transformation for our clients with solutions for enriching client engagement, navigating risk, optimizing efficiency and generating revenue growth.

$6+
billion revenue as in FY23

$10+
trillion in equity and fixed income trades processed per day

7+
billion customer communications processed annually

40+
global clients for managed services

6
decades of experience in the financial services industry

100+
countries in which securities processing is supported

150
Brokerage firms on our securities processing platforms

98%
client revenue retention rate

Industry Representation

Informing, Educating, and Leading Industry Wide Discussion

Through our commitment to the Financial Markets, Broadridge maintains an expansive representation across leading industry associations and groups.

- Chair, Co-Chair, or participate in 24 different Securities Industry and Financial Markets Association (SIFMA) Committees and Societies
- U.S. Representation Within:
  - The Depository Trust & Clearing Corporation
  - Investment Advisor Association
  - International Securities Lending Association
  - The Risk Management Association
  - Major Mailers Association
- International Representation Within:
  - Portfolio Management Association of Canada
  - CDS Financial Administrators
  - CCMA – T2
  - Canadian Exchange Traded Funds Association
  - Investment Industry Association of Canada
  - Futures Industry Association
  - Asian Securities Industry & Financial Markets Association
  - Japan Securities Clearing Corporation

“DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT [information and communications-technology]-related disruptions and threats”

- Council of the EU

Why more regulation with DORA?

Secure and Protect

- Securing your infrastrucutre, policies and practices are critical to avoid cyber related fraud

Prevent and detect

- Managing security risk in your interactions and relationships with your counterparties is key

Sahre and Prepare

- Cyber-Attacks on one company in one location can easily be replicated and impacting a whole sector if not more

Digital Operational Resiliency Act ("DORA")

The Digital Resilience Act (DORA) is an EU regulation that entered into force on 16 January 2023 and will apply as of the 17th January 2025 The Digital Operational Resilience Act (DORA) aims to **establish a clear foundation for security and operational resilience** in the **financial services** sector for European Union (EU) financial regulators and supervisors, while also aligning with **other EU measures on cyber security and data**. DORA establishes a **framework** for digital operational resilience in the finance sector by outlining **five key pillars**, which include:

- Information and communication technology (ICT) governance and ICT risk management
- Testing digital operational resilience
- Reporting system for serious ICT incidents
- ICT third party risk management
- European monitoring framework for critical ICT third party service providers

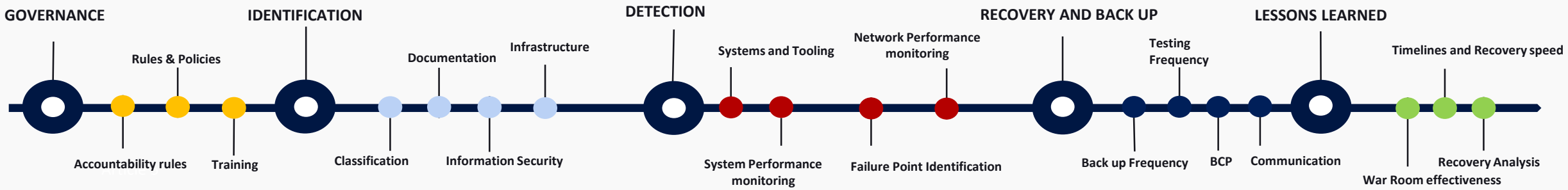
The DORA Objective

- Bringing **critical information and communications technology (ICT)**, including **cloud service providers** (CSPs), within the regulatory perimeter. These would be supervised by one of the European Supervisory Authorities (ESAs), who would have the power to audit, inspect and impose fines.
- DORA aims to harmonise local rules across the EU, setting EU-wide standards for **digital operational resilience testing.**
- Harmonising **ICT risk management rules** across financial services sectors, based on existing guidelines.
- Harmonising ICT incident **classification** and **reporting** and opening the door for the establishment of a single EU-hub for major ICT-related incident reporting by financial institutions.

The Five Pillars of DORA

Financial entities are required to set up a comprehensive ICT risk management framework

ICT risk management framework requirements



DORA

1. ICT Risk Framework	2. Incident Management	3. Testing	4. 3rd Party Risk	5. Information Sharing
Operational risk and Incident Management Recovery and response mechanisms, continuously monitor all sources of ICT risks to establish protection and prevention measures	**Cyber Risk Management** Classification and continuous monitoring and detection of IT risk	**Continuous Threat Led Penetration Testing** Continuous assessments via testing, simulations and Audits (Yearly by independent internal or external auditors)	**3rd Party Risk** Understanding of risk from 3rd Party service providers (Cloud Providers, Technology providers, outsourced Services)	**Resilience and Business Continuity** Established Business Continuity polices and recovery plans Established channels of communication and reporting

Digital Operational Resiliency Act (“DORA”)

DORA requires the creation of a comprehensive ICT Risk Management framework and Digital Resilience Strategy including a comprehensive suite of ICT Risk Management Policies

DORA assessments required to ensure regulatory readiness

- Systems Criticality Assessments (Identify critical assets (In-house & Third-party service provider) which align to critical/important functions)
- Risk and Control Gap Analysis (Map your people, processes, technology, facilities and information that supports your important business services)
- Business Impact Assessments (Understand the business Impact of cyber threat and set impact tolerances for each important business service)
- Incident/problem management processes and tools for efficient management of ICT events
- Robust incident detection and automated response capabilities to reduce impact/improve resilience
- Operational metrics on critical functions for review against defined risk tolerances
- Monitoring and responding to cyber events (Scenario Testing)
- Regular testing of digital operational resilience

Compliance might be difficult due to:

- legacy in-house technology
- technology obsolescence
- out-of-maintenance solutions

From:

- different providers
- in different countries
- with different service levels
- diverse understanding of what is required

Challenges with tech stack

DORA Readiness assessments

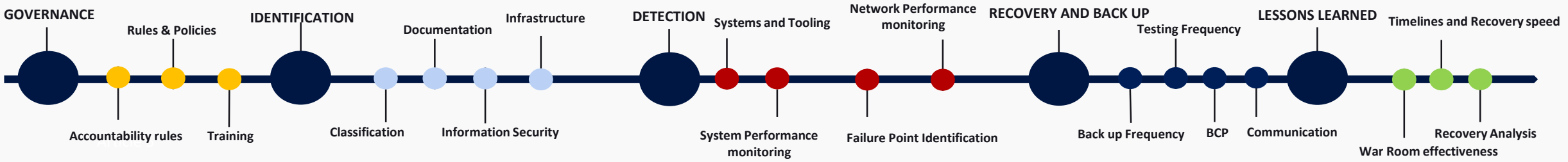
1. Criticality Assessment - Approach & Deliverables

Identify critical digital assets → **Assess impact** → **Prioritize critical assets** → **Develop risk mitigation strategies**

Conduct a criticality assessment to identify and protect your **most important** digital assets and functions. By prioritizing critical assets and developing appropriate risk mitigation strategies, organizations can **enhance** their operational resilience and better withstand potential disruptions and threats.

Current state analysis
It is recommended to analyze the following as part of the assessment:

- **Identification of critical digital assets**: across your entity/enterprise identify critical assets (In-house & Third-party service provider) which align to critical/important functions. Integral to this analysis is the operational model, processes and procedures that underpin and support the services that the critical assets deliver to the business
- **Impact analysis:** Analyze and assess the potential impact of a cyber-attack or major disruption on critical assets and the subsequent impact on operations and clients. This analysis will feed into current planning and communication strategy for such events to highlight existing gaps and vulnerabilities
- **Prioritization:** Based on the asset identification and impact analysis, determine the risk that is presented should a critical system suffer disruption. This will allow you to perform specific risk assessments based on the organization's risk appetite against the firm's strategic objectives to obtain a balanced view
- **Develop risk mitigation strategies:** Risk mitigation strategies will be developed to reduce the risks within the critical assets and their eco systems. These strategies will feed into technology change, operational model revisions, third-party agreements and testing cycles



DORA Readiness assessments

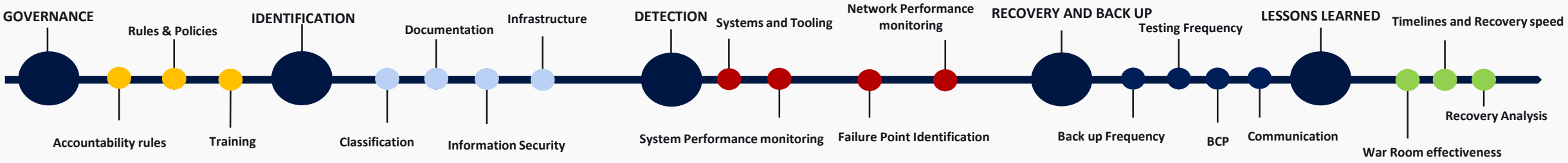
2. Risk and Control Gap analysis

Current State Analysis → **Gap Analysis** → **Recommendations**

Perform a deep dive analysis of your current risk and control framework to identify gaps between current state and target state for DORA implementation. This will require a close examination of the existing risk and control business model with a full review of the ICT risk management and governance process.

Current state analysis
Key activities will include the following:

- **Evaluate and assess the effectiveness of the current ICT change program** to maintain systemic robustness and reduce overall vulnerabilities across critical assets. This will require a deep dive review of past change as well as future change initiatives
- **Analyze the current control framework** that supports critical systems/platforms and their associated support functions. This analysis will help establish the effectiveness of the current model against the DORA future model and identify ineffective or duplicate controls
- **Review current horizon scanning for potential cyber threats** by examining the parameters of the scanning to ensure that it aligns with business risk appetite, perimeter protection levels, data in transit and incoming data streams into the client secure area. Analyze the alert and monitoring processes through metrics and remediation process reviews
- **Understand the current third-party vendor support model for critical functions**, whether it aligns to the regulation and fully complies with DORA standards. Include the third-party vendor industry partners if applicable to allow for effective risk management across the full value chain for each critical service
- **Analysis of resiliency practices**, business continuity policies and disaster recovery plans, including yearly testing of the plans across all supporting functions
- **Assessment of ICT incident management**, internal/customer escalation protocols, monitoring of early detection indicators/controls and reporting procedures for ICT disruptions
- Assessment of employee security awareness training



DORA Readiness assessments

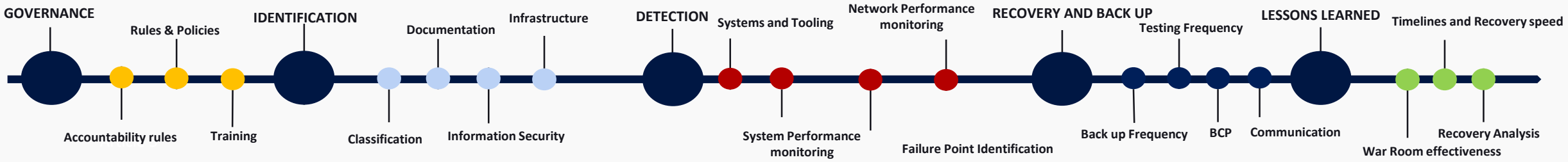
3.Business Impact Assessment

Identify critical functions → **Assess impact & readiness** → **Manage risk effectively** → **Recommend solutions**

Complete a thorough evaluation of the effectiveness and readiness of your business model and review business impact associated with cybersecurity attacks and major Information and Communication Technology (ICT) disruption. This will ensure that your organization is fully prepared to manage cyber risk and achieve full compliance to avoid penalties from the EU authorities.

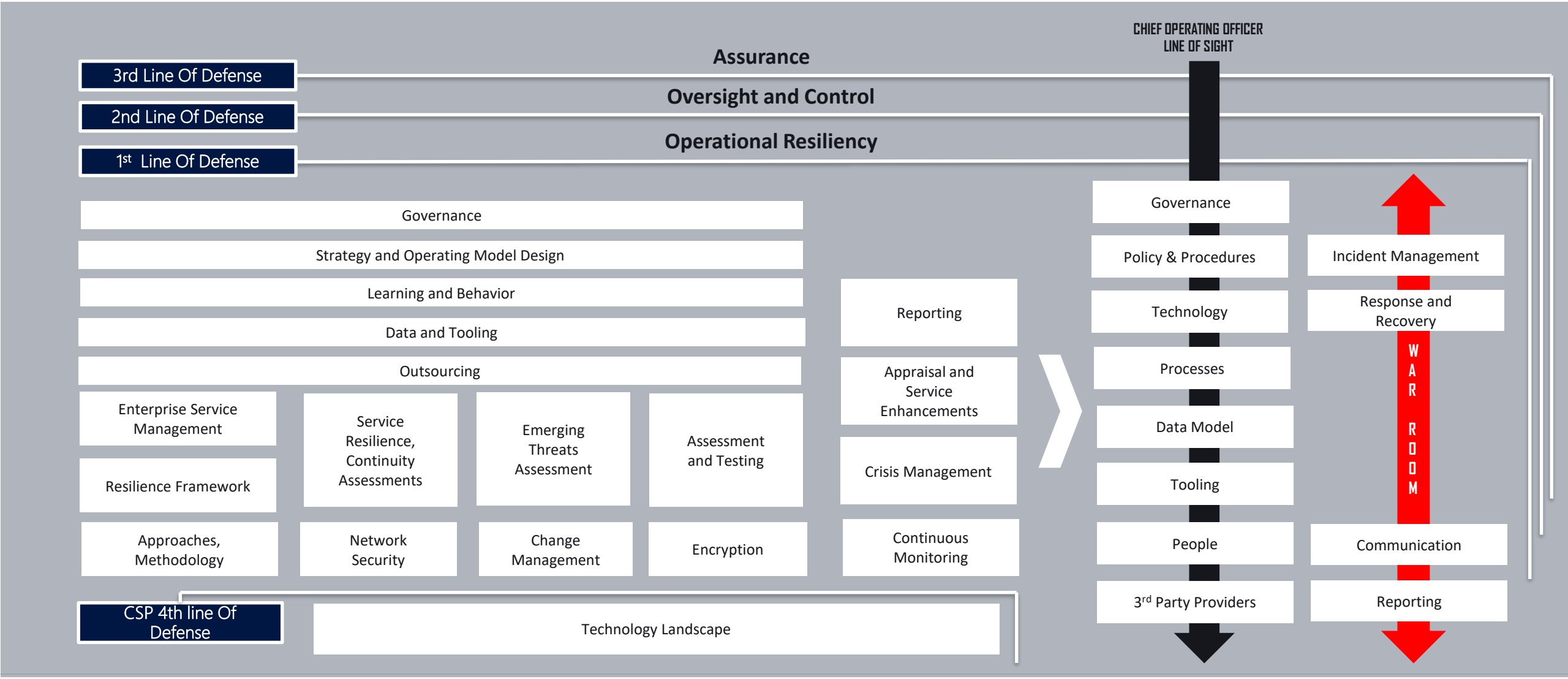
Current state analysis
Key activities will be captured and managed through the following project governance model:

- **Creation of a Service map** from source for critical and important platforms and applications to identify weak points and highlight potential technology upgrade or investment needs.
- Work with technology partners to understand all parts of the Technology stack that could be impacted by DORA and create a detailed checklist of all available and/or missing services
- **List and understand all third party (TP) dependencies** and provide recommendations to monitor their service delivery quality and performance i.e., service questionnaire, SLA agreements
- **Create business case scenarios** for all major event types to assess the current state of readiness and map all risks and controls associated to it including recommendations for remediation i.e., better technology protection, new vendor connectivity, increased resourcing, deliver options paper etc..
- **Perform criticality assessment per function** with full RAG status and detailed action plan
- **Write testing plans for scenario-based testing** to ensure effectiveness of major incident management (cyber threat, ICT management, global system impact, trauma event, BCP failure)
- **Define and assign roles and responsibilities** for the internal teams to closely manage post trauma events and enforce a robust governance model



Digital Operational Resiliency Act ("DORA")

Assess and Validate your entire ICT Operating Risk Framework



Broadridge

Ready for Next

Asset Servicing Automation 2024

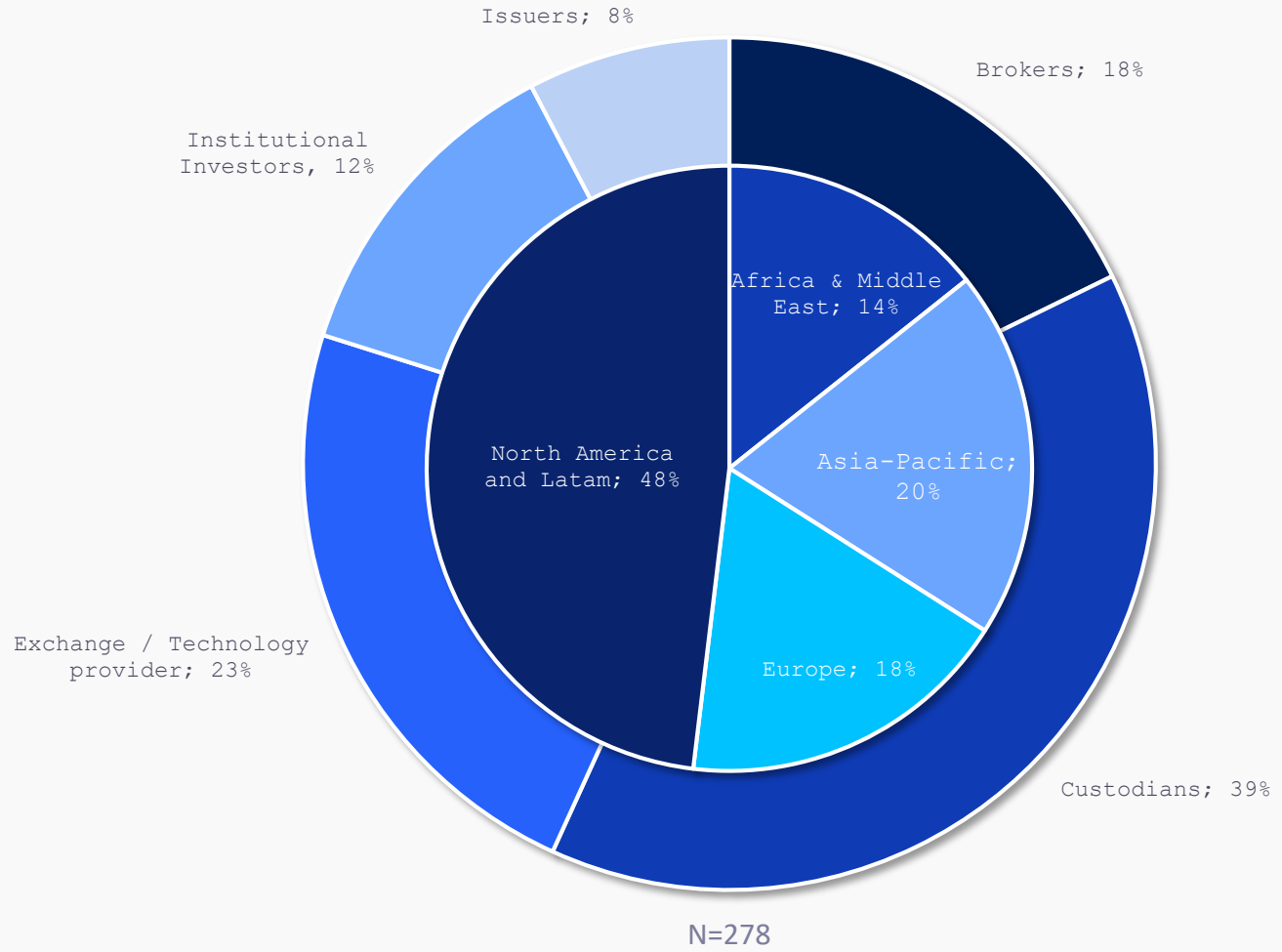
Regulation as the opportunity to innovate

Key Survey Findings

November 2024

Overview

Asset Servicing Automation 2024



Source: The ValueExchange

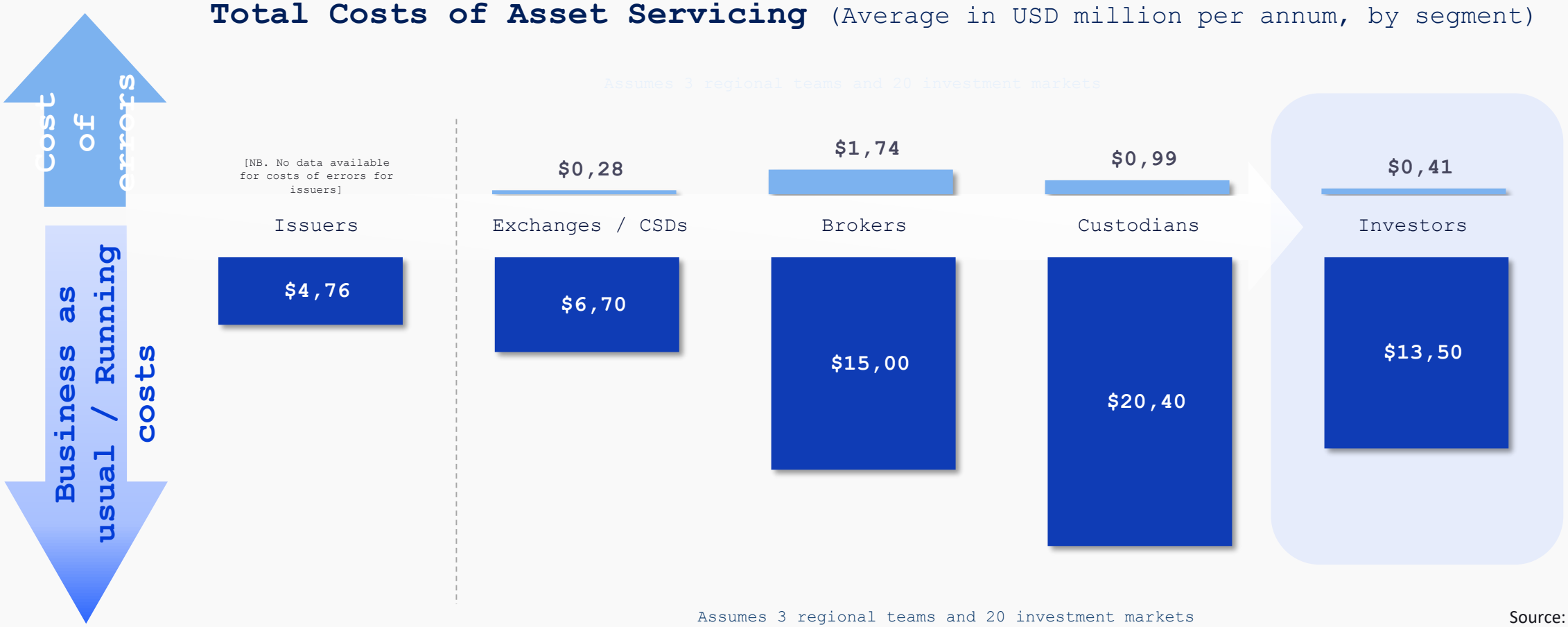
Key Themes

1. **How much** are corporate actions **costing us** in 2024?
2. What **root causes** are we seeing trigger issues across the market?
3. **What steps** are firms taking to minimize cost and risk?
4. What is the **longer-term case** for industry standardization from issuer to investor?

1. How much is Asset Servicing **costing us**?

Fund managers and beneficial owners are carrying a direct cost of USD14m per annum – with indirect, pass-through costs multiple times that value

Total Costs of Asset Servicing (Average in USD million per annum, by segment)

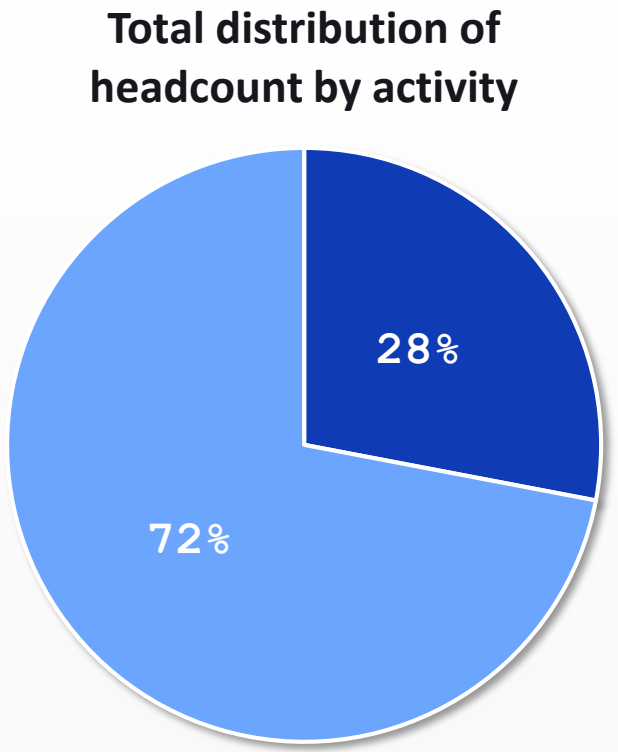


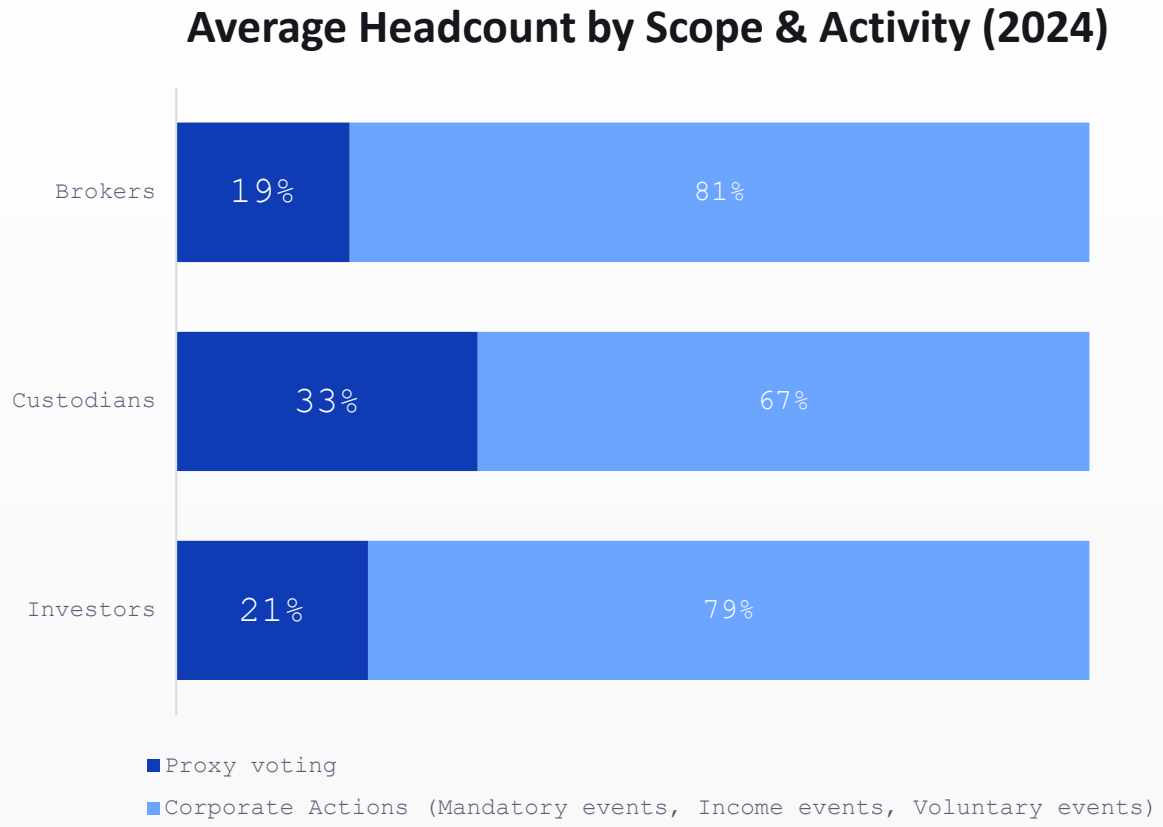
Assumes 3 regional teams and 20 investment markets

Source: The ValueExchange

1. How much is Asset Servicing **costing us**?

Brokers are carrying the heaviest resourcing weight for Corporate Actions processing

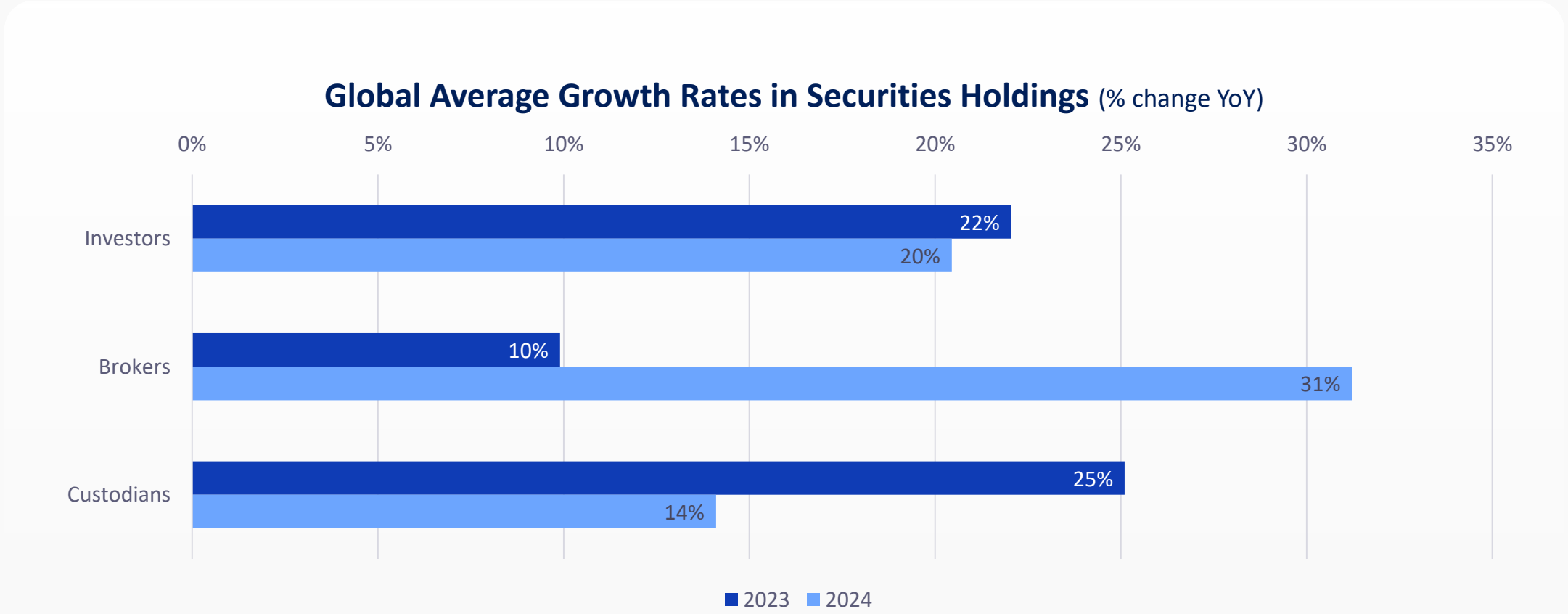




Source: The ValueExchange

1. How much is Asset Servicing **costing us**?

Consistent volume growth is a core part of investors' costs – but do brokers need to be watching out?

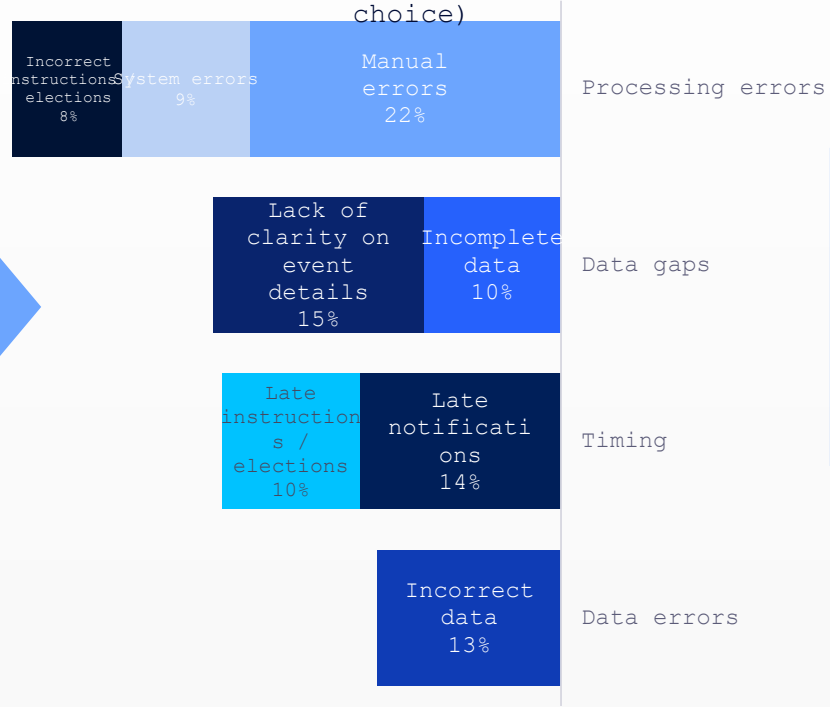


Source: The ValueExchange

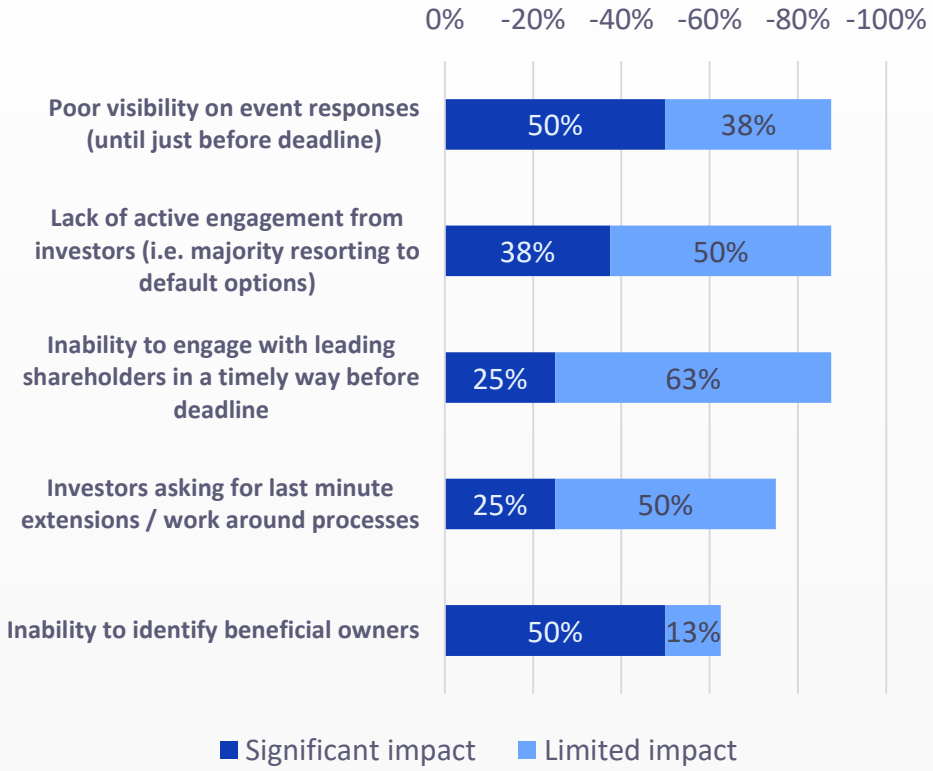
2. What are the **core issues** that we need to address?

Poor automation of data is creating meaningful issues

Manual data processing is creating a range of issues…



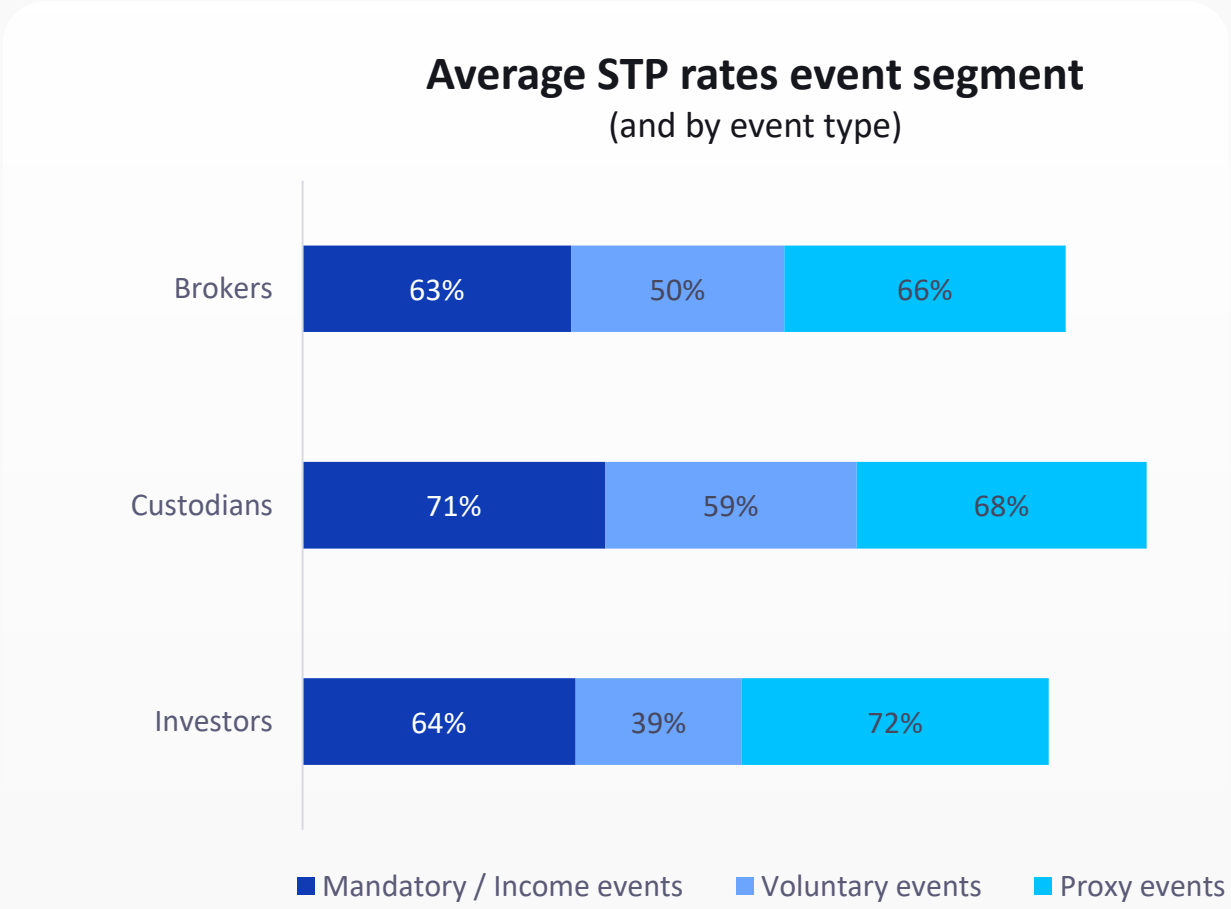
…each of which costs valuable **time** for issuers

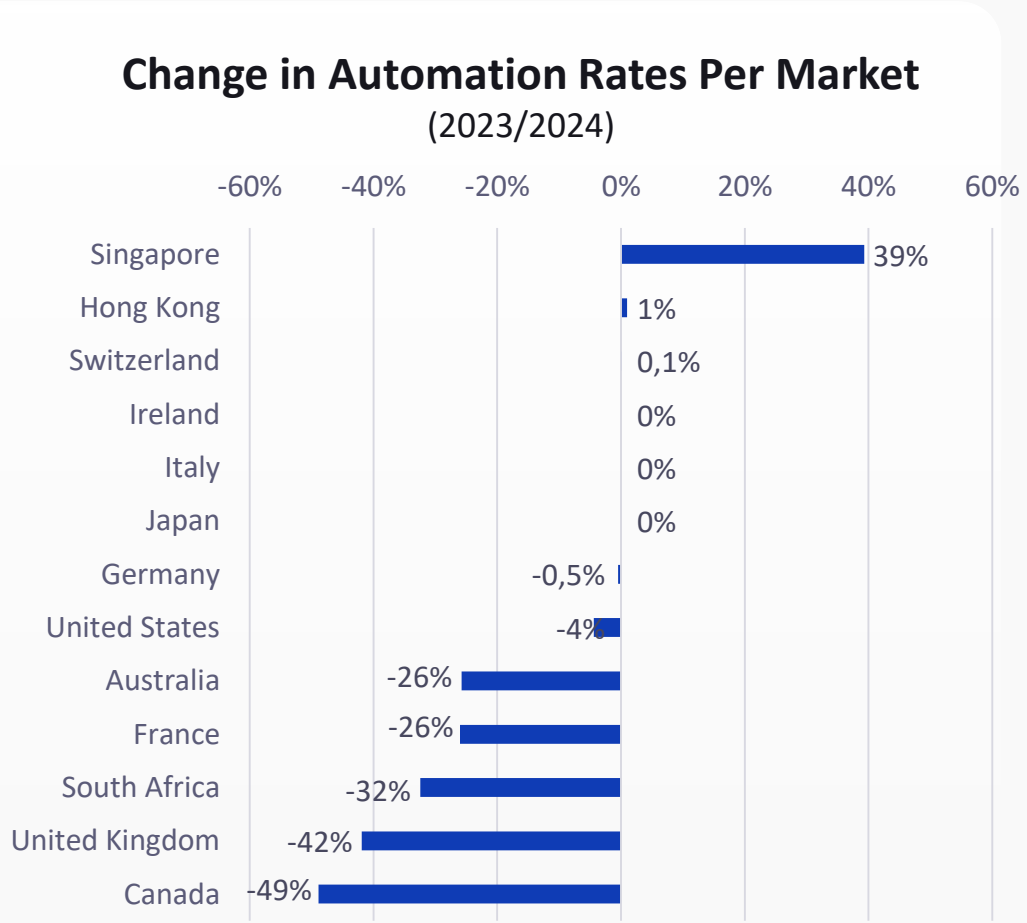


Source: The ValueExchange

2. What are the **core issues** that we need to address?

Our STP rates are low and declining





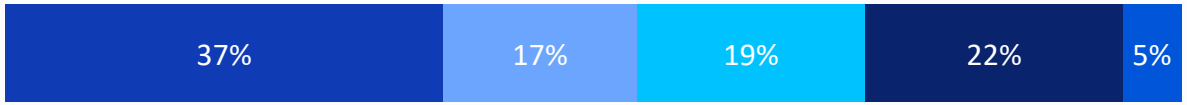
Source: The ValueExchange

2. What are the **core issues** that we need to address?

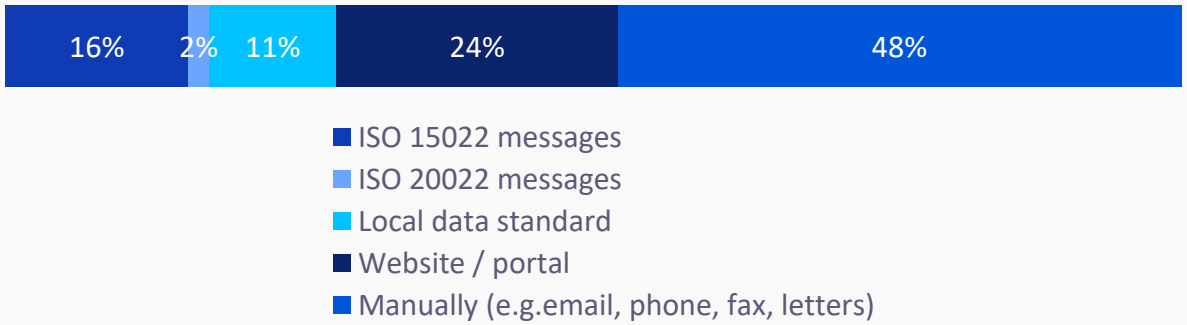
Manual risk is much higher for instructions than for announcements

How are we receiving event notifications

(% distribution, globally)

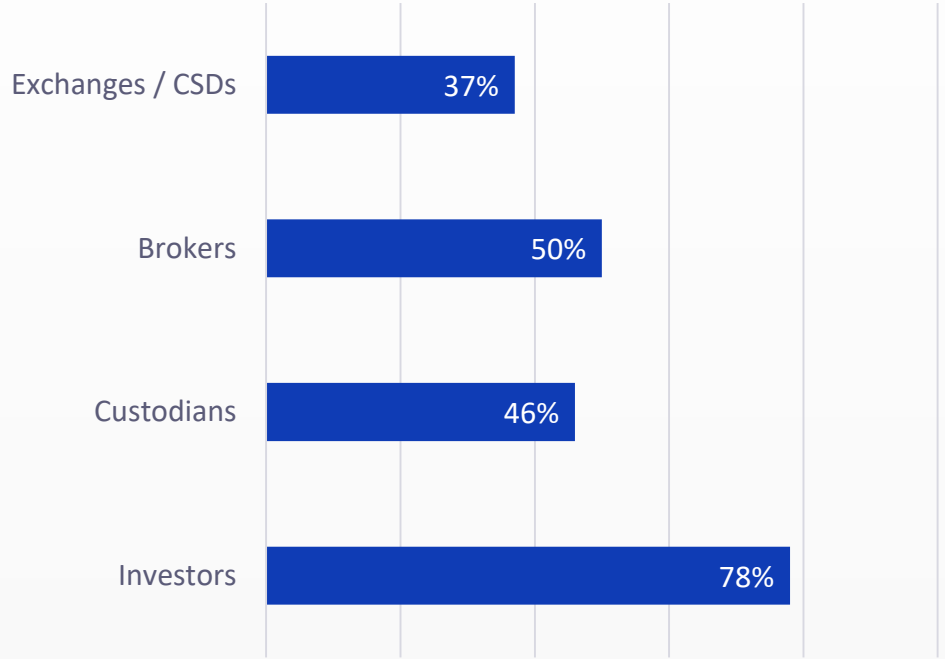


How are we receiving event elections / instructions (% distribution, globally)



How are we receiving event elections

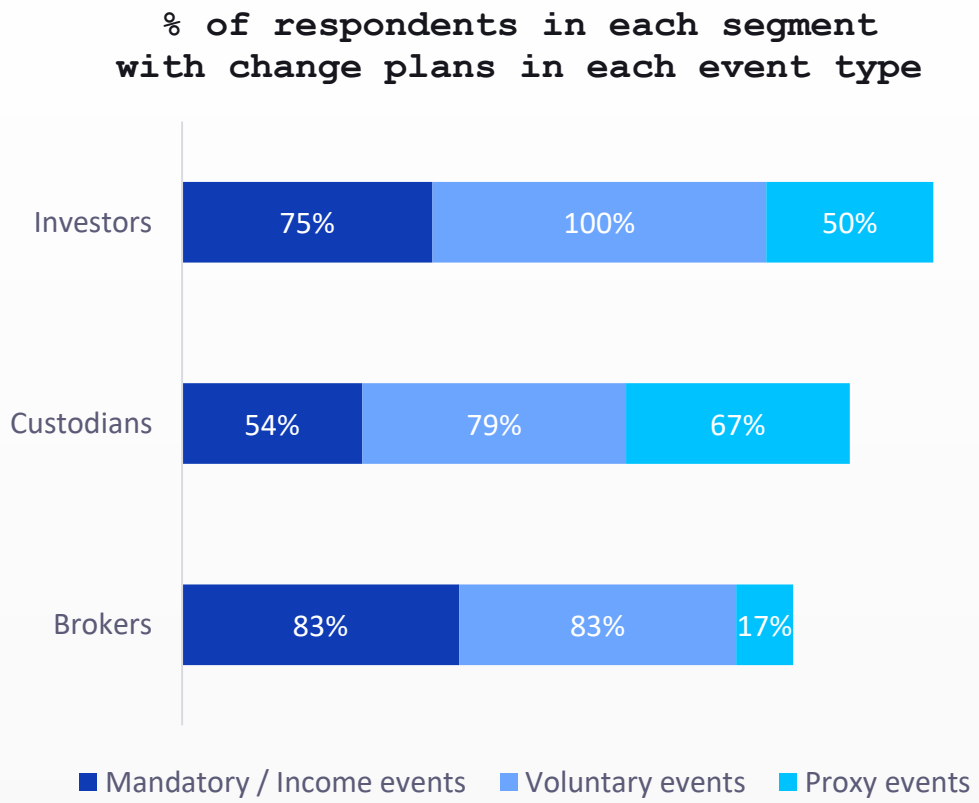
(% receiving manual event instructions, per segment)

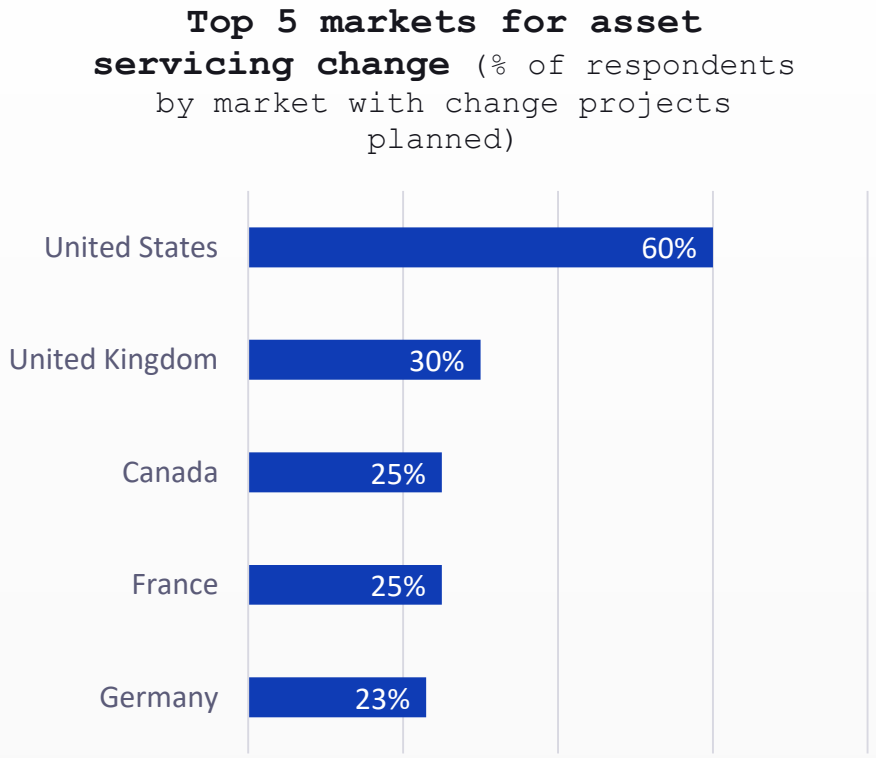


Source: The ValueExchange

3. Where are we driving **change**?

We are spending a lot of money trying to fix voluntary events today

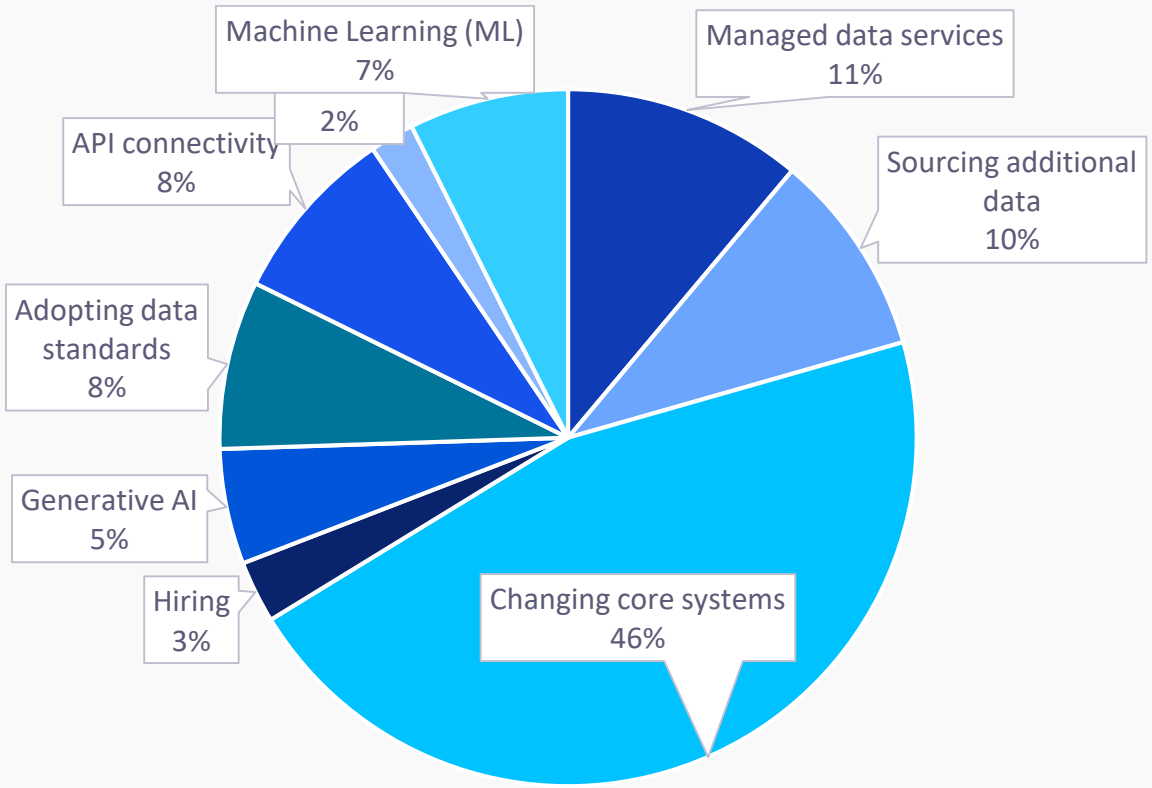


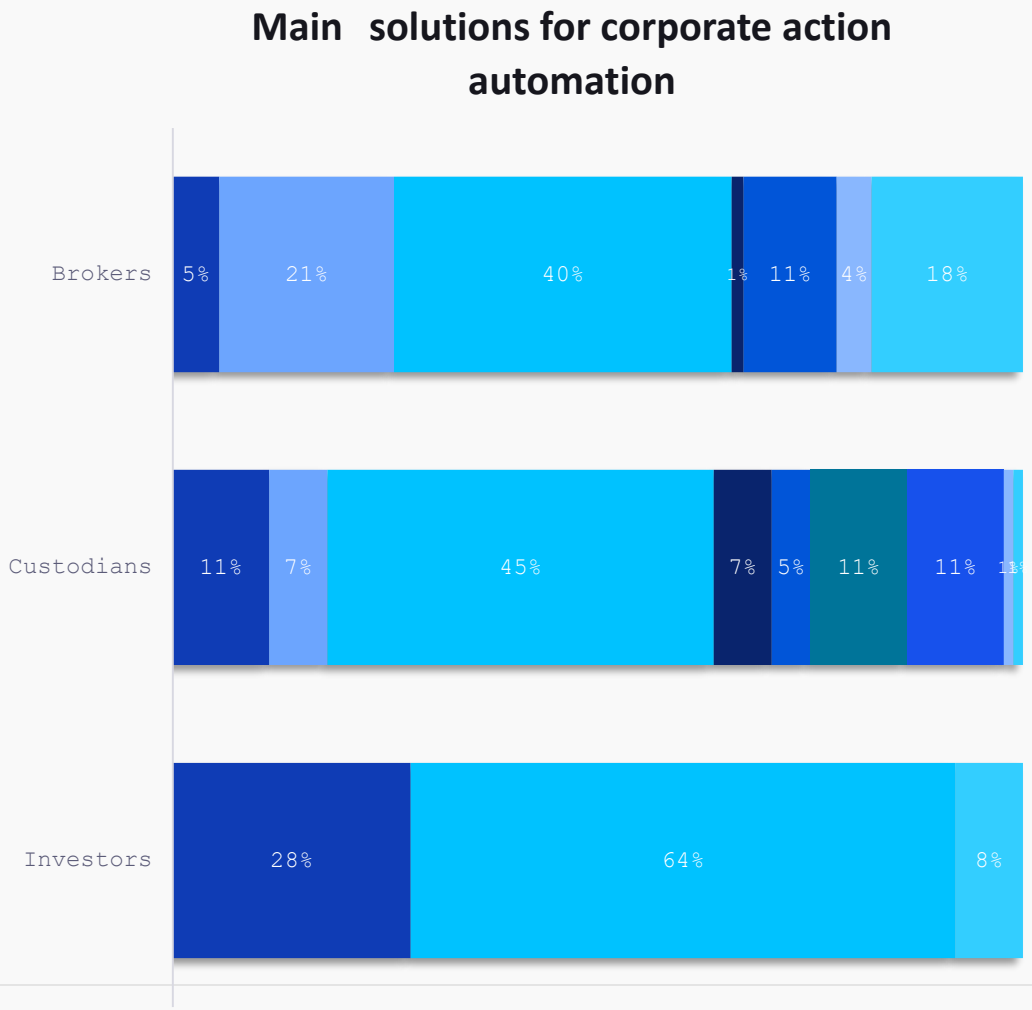


Source: The ValueExchange

3. How are we driving **automation**?

System change and data are our core answers



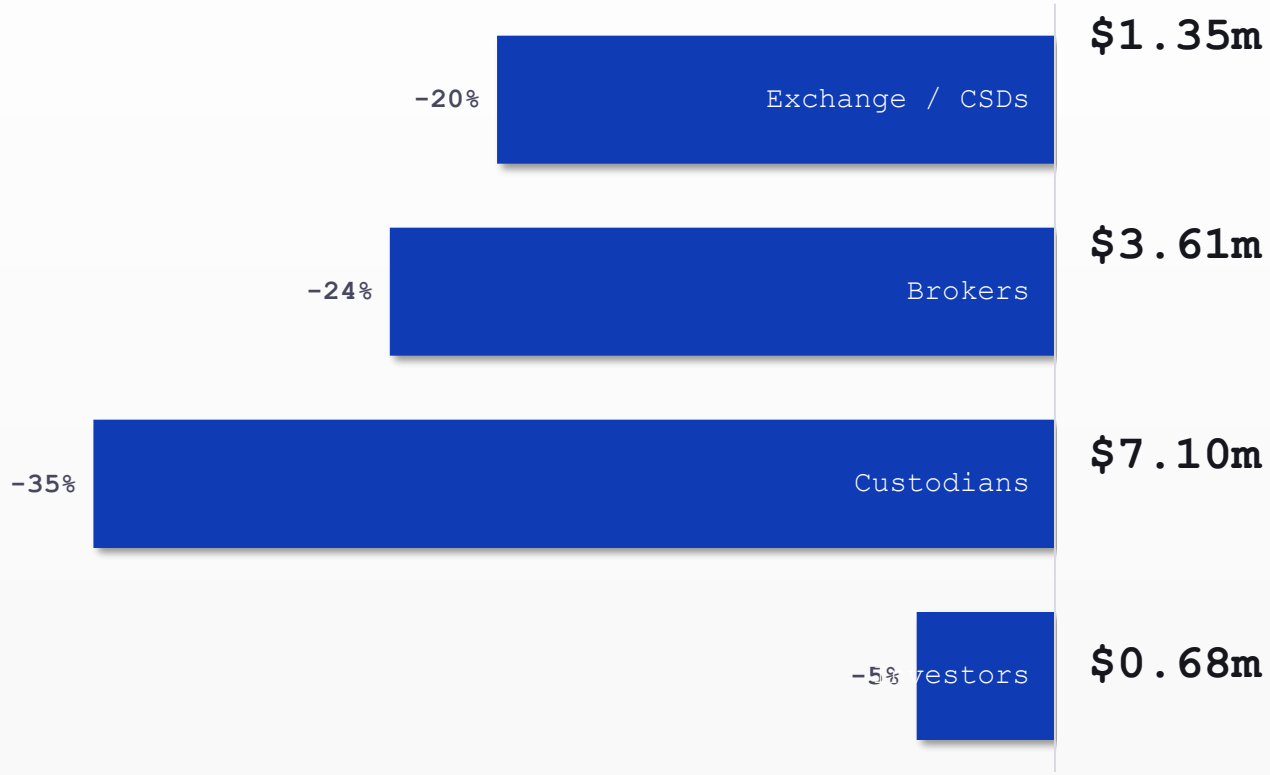


Source: The ValueExchange

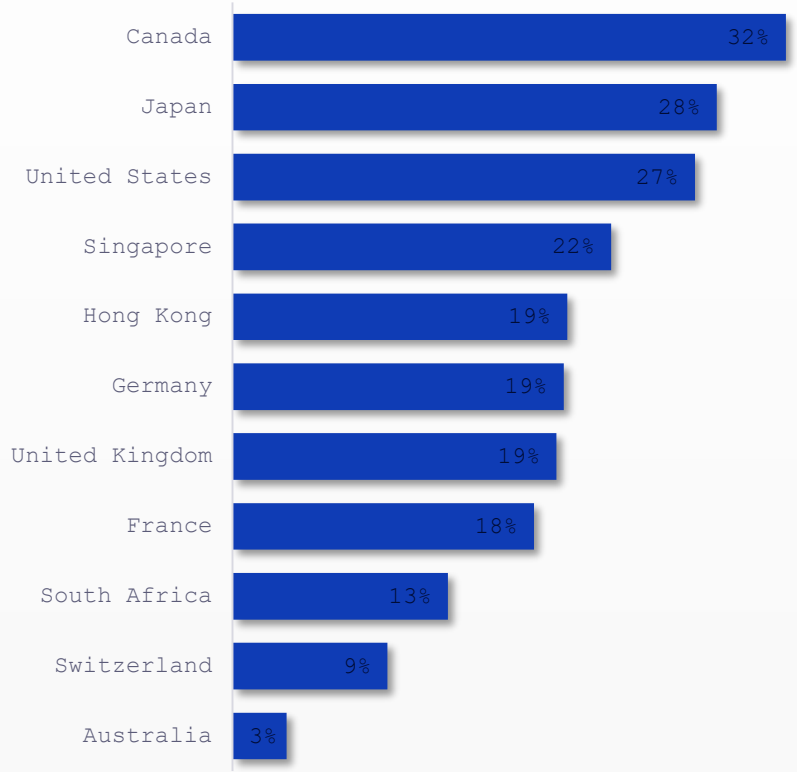
3. What is the case for **logicized event data**?

USD 680,000 per annum removed from investors' direct costs – with several times that in indirect costs eliminated

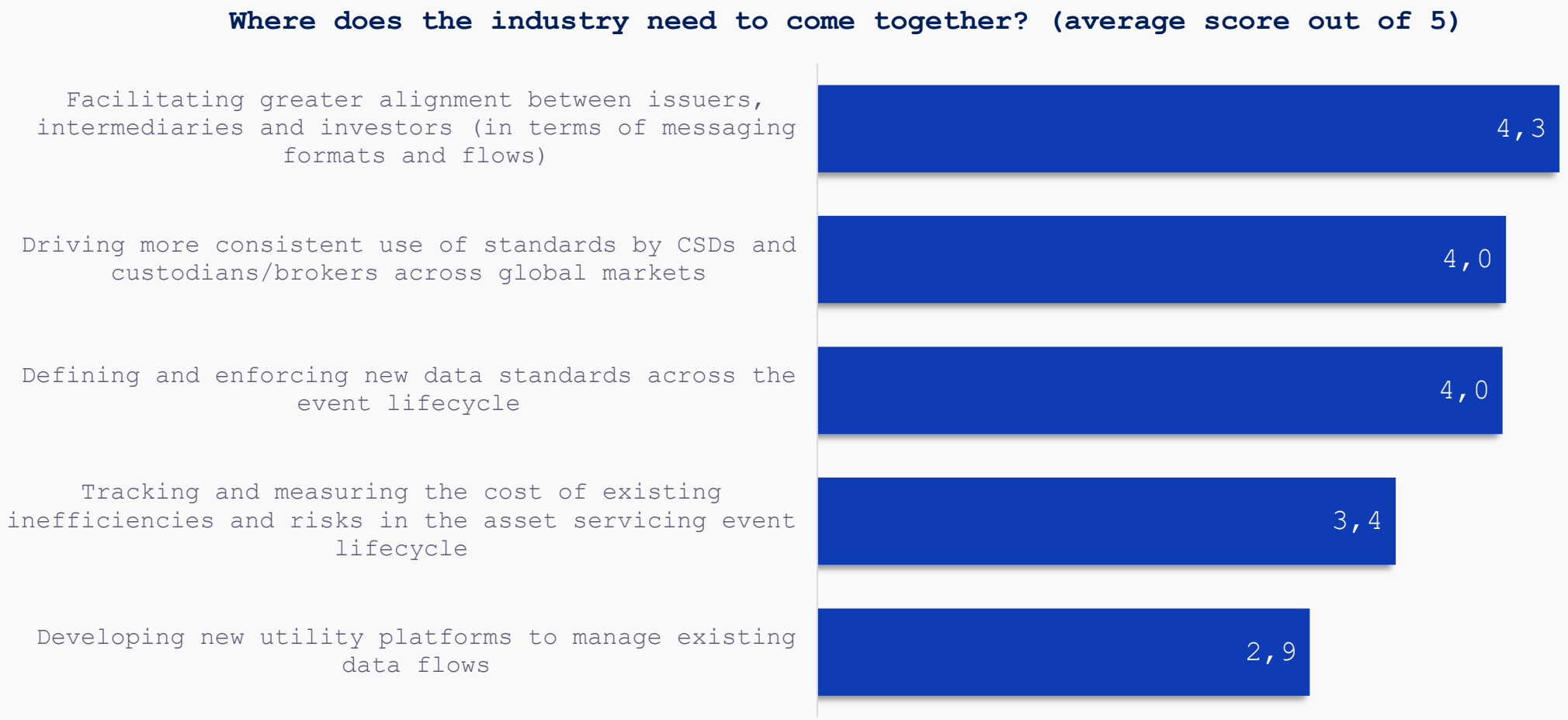
Expected savings from a real time, logicised data feed (% and USD million per firm, per annum)



Expected P&L savings by country (% saving per annum)



4. Where does the industry need to **come together**?



Source: The ValueExchange

Broadridge

Ready for Next

Herzlichen Dank für Ihre Aufmerksamkeit