CAPCO

CHALLENGES, CONSIDERATIONS AND RECOMMENDATIONS FOR MANAGING NON-FINANCIAL RISK ACROSS A CHANGE PORTFOLIO

a wipro company

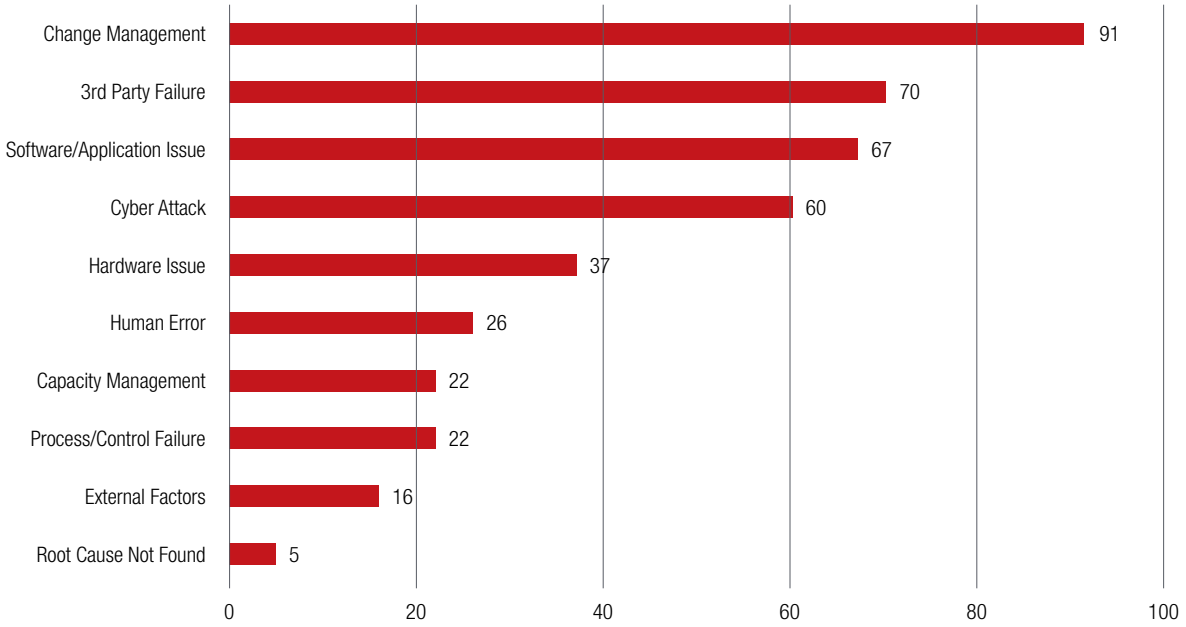
While many financial institutions consider their 'business as usual' non-financial risk frameworks to be reasonably mature, insufficient consideration is often paid to managing non-financial risk within transformations – particularly large-scale programs – in today's fast paced and technology/digital-driven business environment. When it comes to delivering significant transformation programs at pace, financial institutions seldom apply adequate rigor and SME focus when identifying, assessing, or managing their non-financial risk exposures, such as regulatory compliance, financial crime, legal, resilience and cyber.

The COVID-19 pandemic has accelerated increases in the scale and breadth of automation, digitalization and offshoring as well as the reliance on third-party service providers within the industry and has consequently amplified these risks. Headline making failures such as the TSB integration[1] have underlined the importance of robust transformation risk management disciplines and the need to avoid customer detriment, regulatory censure and, in some instances, breaches of local law both during and post program implementation.

In this paper, we outline the principal challenges and pitfalls we've seen financial institutions experience when managing non-financial risk (in both Agile and Waterfall change deliveries), as well as examining key recommendations to ensure expedited delivery and robust risk and control management during large scale transformation.

IT Incidents in the Financial Services Sector, Oct 17 - Sep 18

Incident data ref: parliament.uk publication



The 2019 Parliament Report[2] identified the largest cause (22%) of IT incidents in the financial services sector was related to change management.

1. Megaw, N. (2018). FCA to launch formal investigation into TSB's IT failure. Retrieved from https://www.ft.com/content/a000d194-68a6-11e8-8cf3-0c230fa67aec
2. House of Commons Committee (2019). IT failures in the Financial Services Sector. parliament.uk .

CHALLENGES FACED IN MANAGING NON-FINANCIAL RISK ACROSS A CHANGE PORTFOLIO

We see five key challenges that typically arise when managing non-financial risk across a change portfolio. Left unaddressed, these can lead to delayed delivery, opportunity cost related to manual work arounds, risk incidents, and even customer detriment and regulatory censure.

1. An Inconsistent and Unconnected Approach to Delivery and Risk Management

Different methodologies and interpretations of solutions across disciplines such as program management and risk management can give rise to misaligned stakeholders. For example, if programs adopt an Agile approach to delivery but risk SMEs adopt a Waterfall style when reviewing/challenging, this can cause delays to endorsements, require rebuilds to align with risk appetite, and consequently hinder the pace and safety of product deployment to market. As such, an aligned partnership approach based on agreed principles must be established at the outset to balance effective management of delivery and risk.

2. Inadequate Business Ownership & Unrepresentative Engagement

Risk management is more effective when there is deep buy-in from the business, with a holistic representation of key stakeholder groups and senior management setting the 'tone from above'. If this is absent, the result can be inadequate prioritization of delivery versus risk requirements, poor risk decisioning processes and suboptimal product development, leading to unnecessary remediation work, duplication of effort and delayed or partial deployments. For example, global programs lacking appropriate engagement with country stakeholders can result in local nuances – such as employment law, data privacy, third party vendor requirements or long engagement lead times with regulators – being missed. Furthermore, as products transition from program to business as usual (BAU), executives will be responsible for ensuring risk considerations are met so it is imperative they understand the related risks, controls and implications and effective governance structures are in place to monitor these.

3. Ineffective Risk Governance Framework

Transformation risk governance frameworks often lack the maturity and resourcing power of BAU risk governance frameworks. A lack of effective transformation risk governance can lead to an inability to keep pace with the fluidity and speed of delivery in an increasingly automated, digital world of Agile sprints. Without a nimble and fluid risk governance framework to manage non-financial risk associated with change, the organization could expose itself to myriad risk issues such as cyber-attacks, customer fraud, information leakage, data privacy or conduct concerns. This is especially important in instances of event driven and strategic change designed to capitalize on market opportunities. Recent examples include capitalizing on the Paycheck Protection Program in the US or the Recovery Loan Scheme in the UK, where pace to market is essential. Such environments often present limited time for comprehensive risk analyses and therefore require robust risk acceptance governance processes to ensure senior management visibility, that solutions remain within the scope of risk appetite, and that any post deployment backlog commitments are duly delivered to closure.

4. Conflicting Priorities, and a Lack of Strategic Direction

Lack of transparency and direction during delivery makes risk management more difficult. Without clarity on the program, product or solution end state design or ambition, risk teams often critique partial designs reactively and in silos rather than providing SME counsel proactively and holistically. Strong program partnership with risk teams and clear direction can provide a unified runway and prioritization schedule, enabling optimal use and alignment of resource capacity and reduce multiple re-reviews of each development within the same product.

5. Lack of Understanding, Content, and Appreciation of Risk

Far too frequently, transformation risk may serve as an afterthought within change programs heavily geared to focus on delivery risk. As a result, risk teams tend to be engaged post solution design and either to provide pre-deployment validation or once an incident has occurred. This regularly leads to unexpected remediation exercises being mandated – at the cost of budget and resource which otherwise could have been spent on program delivery – or poor internal or external customer outcomes. This issue becomes especially acute when particular risk themes, such as cyber, cloud, third party, resilience, and conduct, require advanced SME knowledge to ensure viable and sustainable solutions are developed.

EXAMPLE CONSIDERATIONS WHEN MANAGING NON-FINANCIAL RISK ACROSS A CHANGE PORTFOLIO

To ensure non-financial Risks are managed effectively across a change portfolio, an organization should have a strong awareness and understanding of what key risks are applicable to their planned deployments. Below are some examples of key themes and considerations across the risk spectrum that should be front of mind when firms embark on large scale change.

Theme	Example Considerations		
People & Outsourcing	Employment Law & Union Notifications	Employee Comms & HR Engagement	Service Catalogues & Role Transitions
Compliance	Information Handling, Barriers and Control (including Material Non-Public Information)	Data Sharing Agreements	Access Management & Permissioning
Regulatory Bodies	Central Bank notifications	Regulatory Approvals	Independent Assessments
Data & Information Sharing	Data Retention & Storage	Data Hosting	Data Types & Classifications
Finance	SOX	CASS	Local Tax Law
Legal	Terms & Conditions, Enforceability	Cross Border	Data Privacy
Resilience Risk, Cyber & Information Security	Business Impact Assessments	Third Party Risk Reviews	Application Security & Penetration Testing

RECOMMENDATIONS AND SOLUTIONS

Effective management of non-financial risk across a change portfolio requires fluid and nimble (but robust) risk governance to keep pace with the speed of change, supported by deep business and content led Risk Steward engagement, quantifiable risk metrics, and upfront showcases and demos. This, combined with ongoing thematic reviews and horizon scans can provide the organization with a holistic view of its risk profile and position themselves to effectively manage risk. throughout.

- **Fluid and nimble risk governance**

  To enable effective and timely risk management, a fluid and nimble framework is required to keep pace with fast delivery and speed of build in an increasingly digital world. An embedded change team specializing in transformation risk can act as a conduit and fulcrum between risk SMEs, business, and program to remove key blockers and support timely go live. An embedded team which can bridge the gap and 'speak the language' of both the program and risk SMEs can help avoid unnecessary delays to endorsements, drains to SME capacity and reduce reworks required. Furthermore, centralized governance and management of the risk landscape (e.g., risk registers, conditions, approvals, risk acceptances, issues) will enable more holistic assessment across program components and provide business owner comfort when adopting change into BAU.

- **Horizon scanning and early identification of local nuances**

  Program deliveries are becoming increasingly ambitious in nature and depending on the materiality of the change, may require regulatory oversight and/or approval. To ensure timely and risk managed go-live, it is prudent to front run potential regulatory considerations ahead of schedule to anticipate local nuances, such as cloud hosting and data sharing restrictions in particular markets. With upfront early assessment and sign posting of local requirements and implications, unexpected delays to go-live can be avoided and risk and control solutions can be designed and factored into the build from the outset. Clear engagement plans and accountability for local stakeholders and SMEs should be devised to ensure compliance to policy, local regulation, and laws.

- **Early and iterative showcases, demos, and overviews**

  Upfront initial risk engagement and partnership from program and business will bring risk teams along the journey and provide a platform for holistic risk assessment. Regular, nimble governance forums catering for showcases, demos and overviews will facilitate the early identification of risks and SME input into mitigants and control solution design. Upfront showcases of scope can also determine whether further specific SME content knowledge is required, such as for cyber risk and platform resilience related themes.

- **Metrics, tooling, and testing**

  Quantifiable risk insights will provide stakeholders including senior management with data driven insights, visibility, and comfort that delivery meets design requirements and risk appetites throughout the program lifecycle. Metrics will support risk based decisioning reflective of impact and enable enhanced balancing of risk versus commercial benefit. Tooling and routing rules for endorsements and relevant SME signoffs, such as for data sharing agreements, can be automated and simplified to enable effective and efficient review of risk items by the necessary persons first time. Risk SMEs engaged in testing post development will ensure risk concerns have been remediated and deliverables remain within risk appetite.

- **Deep Business engagement & ownership**

  With key senior buy in and appropriate 'tone from above', understanding and appreciation of risk within the first line can advance, and deployment accelerated. When the business is brought along the delivery and risk management journey and engaged with risk SMEs, local nuances, such as country specific regulation, understanding culture and practice as well as stakeholder identification and management, can be navigated more effectively. Delivery and non-financial risk should be seen and managed as two sides of the same coin.

- **Thematic reviews and impact assessments**

  With large scale complex change, thematic reviews and impact assessments can provide comfort to senior management and risk SMEs that the organization is compliant with policy and local regulation. Some programs may involve a heavy digital and or tech component, prompting the need for third parties and IT development. As such, deep dives such as third-party risk assessments, application security reviews or penetration testing can identify potential risk considerations like inadequate licensing or cyber security deficiencies. Such reviews can provide senior management teams with rich insights to product performance and customer feedback throughout the product lifecycle, both pre deployment and at periodic intervals (e.g. following volume increases, new market rollouts or wider system integrations).

- **Risk SMEs and Emerging Technologies**

  As the risk landscape continues to evolve and new and emerging risks arise at increasing pace, having the right level of risk subject matter expertise integrated into your program is critical. With unrelenting technological disruption and the increased use of solutions such as cloud and AI, new risks have come to prominence that require specialized knowledge and experience to navigate effectively. Content rich Risk SMEs with a detailed understanding of the technology, the vendors, the risks, and the controls are central to enabling an organization to manage its transformation risk exposure effectively. In today's world, Non-financial risk management requires more than effective governance and engagement – SMEs who really understand and can guide business units on the risk associated with technology and change are essential.

LOOKING AHEAD: RISK MANAGEMENT OF DIGITAL TRANSFORMATION, AGILE DELIVERY AND BRIDGING THE DIVIDE

The 'Fourth Industrial Revolution'[3] we are now experiencing will gift opportunities such as increased use of digital, robotics, AI, and computing technology to support the financial sector. However, with new opportunities come the development of new risks which may not be front of mind or fully understood, with the FCA reporting that of all customer-facing incidents in 2019, 7.4% had a root cause relating to change activity[4]. The increasing requirement to deliver change at pace across large scale transformation and digital programs is the 'new normal' and has given rise to a need more than ever to put a 'risk wrapper' around change. A risk management wrapper with an embedded program risk team can bridge the gap between program philosophies and stakeholders, provide comfort to Management that risks are being adequately managed, and provide valuable risk insights to support future program strategy.

How Capco can support robust non-financial risk management across your change and transformation programs:

- Through our deep knowledge and focus on the financial services industry, experience of large-scale program delivery and record of delivering change in collaboration with clients and third-party suppliers, we understand what is required to deliver organization-wide change management programs effectively.
- Capco can embed dedicated, nimble teams with specialist skills, frameworks and tooling across Risk Management, Data, Digital, Transformation and Agile attuned to accelerate robustly controlled delivery.
- Our track record in using data insights, analytics, and technology to deliver similar programs of work and ability to mobilize quickly can support organizations to both proactively and reactively manage non-financial risk. This ensures the development of sustainable, robust solutions, reducing likelihood of disruption in crisis, greater compliance with incoming regulations and greater customer satisfaction.

3. Schwab, K. (2017). The Fourth Industrial Revolution. Portfolio Penguin; 1st edition (5 Jan. 2017).
4. FCA. (2021, 02 05). FCA.org.uk . Retrieved from https://www.fca.org.uk/publications/multi-firm-reviews/implementing-technology-change#lf-chapter-id-the-impact-of-change-incidents

AUTHORS

Evert Bekker
Michael Briffa

CONTACT

Stephen Watts
Partner
Stephen.watts@capco.com

Tom Leach
Partner
Tom.leach@capco.com

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company