Risk category	COVID-19 Audit Area	Rationale
Regulatory risk	Compliance monitoring	Remote working of an entire workforce decreases the ability for firms to fulfil operational compliance monitoring activities, especially in relation to the recording of calls, e.g. trade compliance, recording of customer call centres.
	Conduct risk	Firms have been asked by the FCA to support customers during this challenging time. Some customers will be experiencing financial hardship and may struggle to make mortgage and loan repayments; likewise, some insurance product lines will see an increase in claims – whatever the example, firms need to ensure that they are being flexible, fair and compassionate to customers.
	Fund liquidity	Some funds are facing increasing difficulty in meeting investor redemptions, typically borne out illiquid asset classes.
	Regulatory reporting	The ability to meet regulatory reporting deadlines will be under strain during this period. Proactive regulator communication will be important.
Financial risk	Liquidity management	Financial Institutions have been returning capital to shareholders over the past few years. The recent market stress may put liquidity pressure on firms, which may want to preserve capital by halting or reducing dividends and share buybacks. Liquidity is likely to tighten, causing firms to invoke contingency funding plans. Real-time cash flow forecasting is critical at the moment. In addition, market volatility could result in large swings in stress testing and limit / solvency appetite breaches.
	Counterparty credit risk	Recent market events may have affected counterparty credit profiles.
	Capital management	Risk-weighted assets may be impacted by higher charges from increased volatility levels and higher counterparty risks.
	Revenue and cost management	The COVID-19 induced economic environment is likely to lead to a reduced demand for financial services products, causing a depression of net revenue. The immediate impact will be on AUM linked revenue sources and real estate investment portfolios, but in the medium term, this could knock onto banking and insurance products. Identifying the vulnerable revenue sources and taking early action to reduce costs are key.
	Market risk	A sharp drop in interest rates and increased volatility in securities and FX prices increased market risk, potentially leading to losses.
Operational risk	Brand and business model	How firms engage with and respond to their customers will be a measure of success after the crisis. What does the future business look like post crisis and what decisions need to be made during this time to emerge with strength.
	Talent management	The impact on staff will vary by firm, however, all firms need to identify key persons in business critical roles (developing contingency plans) and should be modelling and closely monitoring the impact of sickness levels on business continuity.
	Accessibility / disability / H&S at work	The rapidly enforced remote working means that employees may not be set up sufficiently at home with Occupational Health determined support (e.g. chair, monitors, etc.).
	Fraud risk	Staff and customers may be facing increased financial hardship, leading to an increased risk of fraudulent activities.
	Outsourcing	Firms will need to be comfortable that business critical outsourcers have sufficient COVID-19 resiliency plans. These will need to be monitored and appropriate contingencies developed.
	Essential programme delays Change portfolio risk	Delays to regulatory or financial reporting standards, e.g. IBOR, IFRS 17, etc. Inappropriate cancellation of "non-essential" change projects/BAU activity leading to strategic & operational business risks crystallising.
Technology risk	IT Infrastructure Capacity & resilience	The immediacy of whole-firm remote working will have created infrastructure and capacity challenges. The bandwidth and resiliency of the infrastructure will be essential to ensuring effective business continuity.
	Cyber Security & data protection/loss	The increase in remote working/ relaxing risk tolerances (e.g. for third parties) significantly increases the vulnerabilities to & impact of an attack. Anticipated significant increase in socially-engineered cyber attacks targeting financial and PII data Uneducated/controlled use of collaboration tools (e.g. Zoom) & home computing (e.g. personal printers) exposes confidential data to inappropriate access and use.