

Cracking the DORA Code

How Digital Twin Will Revolutionise Operational
Resilience in the Capital Markets



Cracking the DORA Code

How Digital Twin Will Revolutionise Operational Resilience in the Capital Markets

Given the prevalence of black swan events this decade – not least the COVID pandemic, the fallout from BREXIT and the Silicon Valley Bank collapse – operational resilience has become a top priority for financial institutions and regulators alike. In January 2023, the Digital Operational Resilience Act (DORA) came into force in the European Union (EU). Under the terms of the legislation, European financial institutions, including banks, investment firms, crypto-asset service providers and critical third-party service providers must implement compliant – and ultimately more sophisticated operational resiliency frameworks than many currently have – before the 17 January 2025 deadline. This calls for scenario testing frameworks that are more accurate than the traditional scenario testing methods commonly used today. One potential approach is to utilise digital twin technology. A digital twin is an AI-based software model that creates an exact, virtual representation of a real-world entity or process. This article will explore how a digital twin can enable firms to model and improve their operational resilience in an offline environment and enhance the effectiveness of their response and recovery plans.

DORA is a broad regulation covering all aspects of operational resilience across all authorised European financial entities, including investment firms, trading venues, crypto-asset service providers and ICT third-party service providers.¹ One of the regulation's requirements for in-scope firms is to perform digital operational resilience testing. Specifically, firms must establish their own procedures to prioritise, classify and remedy all and any issues revealed through the performance of the tests. In essence, firms must ensure that all identified weaknesses and deficiencies are addressed.

GreySpark Partners has observed ambiguities in the DORA regulations and an absence of 'best practice' guidelines for firms implementing a digital operational resiliency testing framework. DORA does not provide guidance on how much firms should aim to spend on cybersecurity, and there is a lack of clarity on the methods that firms should employ to adequately mitigate potential threats.² Consequently, many firms are unsure of what a 'good' operational resiliency framework looks like, leaving them at risk of not achieving full DORA compliance ahead of the 2025 deadline.

Given that UK financial firms have been subject to operational resiliency regulations from the Prudential Regulatory Authority (PRA), Financial Conduct Authority (FCA) and Bank of England (BoE) since March 2022, EU financial firms may be able to glean learnings from the UK experience. GreySpark has observed that UK firms have found it difficult to fit operational resilience into a one-size-fits all framework since each firm faces its own unique challenges. Even so, they have often received less ongoing regulatory feedback and guidance than they would have preferred. This suggests that EU firms could potentially find their own regulators to be less prescriptive about what a firm's compliance with DORA should look like.

Nevertheless, firms are required to press ahead and, under the terms of DORA, they must run comprehensive scenario testing of their security and resilience and fully address any vulnerabilities identified by that testing. Specifically, DORA legislation requires firms to carry out business impact analyses based on 'severe business disruption' scenarios, and fully address all detected vulnerabilities.³ This is likely to increase supervisory pressure on firms to develop more sophisticated scenario testing methods, and to build redundancy and substitutability into the systems that support the Critical Important Functions (CIFs).^{4,5} GreySpark's opinion is that achieving the appropriate level of scenario testing sophistication and precision required under the terms of DORA is likely to only be possible through the use of AI technology. Traditional scenario testing methods, which can be clunky and error-prone, just will not cut the mustard. Additionally, further clarification on resilience testing requirements under DORA is due to be released in Q4 2024, so in-scope firms are essentially required to be compliant with legislation that has not yet been fully outlined.⁶

As **Figure 1** shows, the UK Operational Resilience and DORA scenario testing methods exhibit several key similarities and differences.

Despite DORA's more prescriptive stance, EU financial firms are still largely left to their own devices when it comes to implementing an operational resilience framework. Consequently, firms are likely to utilise one of several types of scenario testing methods, rather than gravitate towards one, standardised approach.

¹ Norton Rose Fullbright. (2023). *Digital Operational Resilience for the Financial Sector (DORA): 10 things to know*. [Online]. Norton Rose Fullbright. Last Updated: January 2023. Available at: <https://norton-rosefulbright.com/en/knowledge/publications/251c1837/digital-operational-resilience-fo> [Accessed 22 November 2023].

² Forkast. (2023). *Why Europe's DORA regulation is a band aid but not a cure*. [Online]. Forkast News. Last Updated: 23 January 2023. Available at: <https://forkastnews/europe-dora-regulation-band-aid-not-cure/> [Accessed 22 November 2023].

³ Deloitte. (2022). *Digital Operational Resilience ACT (DORA)*. [Online]. Deloitte. Last Updated: 5 October 2022. Available at: <https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/ie-risk-advisory-digital-operational-res> [Accessed 22 November 2023].

⁴ Substitutability refers to the extent to which a system or process can take a course of action, be substituted for another, and obtain similar outcomes.

⁵ Critical Important Functions (CIFs), from an operational resiliency standpoint, refer to systems that are necessary to perform activities of core business lines.

⁶ Jina, R. (2023). *Get Prepared for Digital Operational Resilience Act (DORA)*. [Online]. Edgescan. Last Updated: 20 October 2023. Available at: <https://www.edgescan.com/get-prepared-for-digital-operational-resilience-act-dora/> [Accessed 22 November 2023].

Figure 1: Similarities and Differences in UK Operational Resilience and DORA Frameworks

Source: Deloitte⁷, GreySpark analysis

UK PRA and DORA regulations	
 Similarities	 Differences
- Both frameworks expect firms to improve mapping of underlying policies, processes and people that support their core business services, representing a key prerequisite for understanding the knock-on effects of business disruptions. - Both regimes are sufficiently in line with the Basel Committee's 2021 principles for operational resilience. - Both regimes imply that firms should assume that disruption is inevitable in the current macroeconomic and geopolitical climate, and work towards building an appropriate level of resilience.	- DORA takes on a more prescriptive stance than the UK regulations, as it consists of legally-binding legislative requirements for firms. The UK's operational resiliency framework utilises more of a principles-based approach that allows supervisors to use their judgement in assessing potential operational resiliency outcomes. - DORA primarily focuses on the risks arising from ICT disruptions, whereas the UK adopts a risk agnostic approach and is more outcomes-based. - DORA has additional requirements in some areas, including provisions on regulators' oversight of critical third-parties and incident threat reporting/classification. These requirements are currently not part of the UK's operational resilience framework.

⁷ Nair, S and Black, S. (2023). *Implementing the DORA: What EU financial services firms can learn from the UK's path to implementing operational resilience*. [Online], Deloitte. Last Updated: 6 June 2023. Available at: <https://www2.deloitte.com/uk/en/blog/emea-centre-for-regulatory-strategy/2023/implementing-the-dora-> [Accessed 22 November 2023].

⁸ Basel Committee. (2021). *Principles for Operational Resilience*. [Online], Bank for International Settlements. Last Updated: March 2021. Available at: <https://www.bis.org/bcbs/publ/d516.pdf> [Accessed 27 November 2023]

Traditional Approach to Scenario Testing in Capital Markets

Traditionally, financial institutions have taken various approaches to scenario testing, including live production environment testing, internal and external simulated scenario testing and even workshops and team-based drills. However, in 2023, simulations are the most popular approach to scenario testing in financial institutions.

In a simulation, a computer-based programme is used to assess the resilience of a financial firm in a plausible, hypothetical scenario, such as an IT infrastructure failure, for example.

Figure 2 gives some examples of Primary Scenarios tested by financial institutions and how they can be categorised under DORA defined pillars.⁹ Each pillar represents a critical area that a firm needs to ensure is resilient to ensure its overall functionality and continuity.

Evolving regulatory demands are exposing inadequacies in existing simulation-based scenario testing methods, however. One problem with simulations is that they are largely static. In other words, simulations are subject to pre-defined data sets and are unable to incorporate real-time data updates and integrations. Typically, data is input manually before the simulation is run, and as a result, there are limitations on the number of different scenarios that can be simulated, realistically. In addition, simulation testing in financial firms is built largely on cumbersome legacy technology systems and utilises data inputs held in silos. As a consequence, scenario tests can incorporate inconsistencies and mistakes, and accountability can be disputed. Collectively, these factors can lead to a disconnect between business units and drive up scenario testing costs. According to Harvard Business Review, data silos can increase costs by as much as 80%.¹¹

Figure 2: Categorised Examples of Primary Scenarios to be Tested

Source: The Investment Association¹⁰

Pillars	Primary Scenarios
 Operational crisis management	• Inability to deal with multiple significant incidents • Failure of infrastructure to manage a crisis
 People	• Mass staff absence • Lockdown
 Supply Chain & Processes	• Material outsourced service provider failure
 Technology & Information	• IT Infrastructure Failure • National Infrastructure Failure
 Facilities	• Loss of premise supporting key workers
 Cyber & Fraud	• Large Scale Cyber Attack • Large Scale Fraud

⁹ Primary scenarios are specific events that pose a significant risk or threat to a firm's operations within each pillar.

¹⁰ The Investment Association. (2021). *Scenario Testing: Severe but Plausible*. [Online]. <https://www.theia.org/sites/default/files/2021-12/IA%20Scenario%20Testing%20Severe%20but%20Plausible%20Dec21.pdf>. Last Updated: December 2021. Available at: <https://www.theia.org/sites/default/files/2021-12/IA%20Scenario%20Testing%20Severe%20but%20Plausible> [Accessed 22 November 2023].

¹¹ Wilder-James, E. (2016). *Breaking Down Data Silos*. [Online]. Harvard Business Review. Last Updated: 5 December 2016. Available at: <https://hbr.org/2016/12/breaking-down-data-silos> [Accessed 22 November 2023].

Digital Twin Technology

A digital twin is a software programme that creates an exact, virtual representation of a real-world entity or process by leveraging AI techniques. Digital twins are dynamic, in that they are linked to data sources from the real, operational environment and access that data in close to real time. This means that the digital twin immediately reflects any changes to the operational environment. Data outputs from real-world processes are run through the digital twin software, which generates an evaluation. The feedback is analysed and the analysis is tested, so that the process itself is improved and the cycle iterates toward optimality. The result is a hyper-realistic virtual model of a system that can test typical stress scenarios, generated in seconds without the need for significant human intervention.

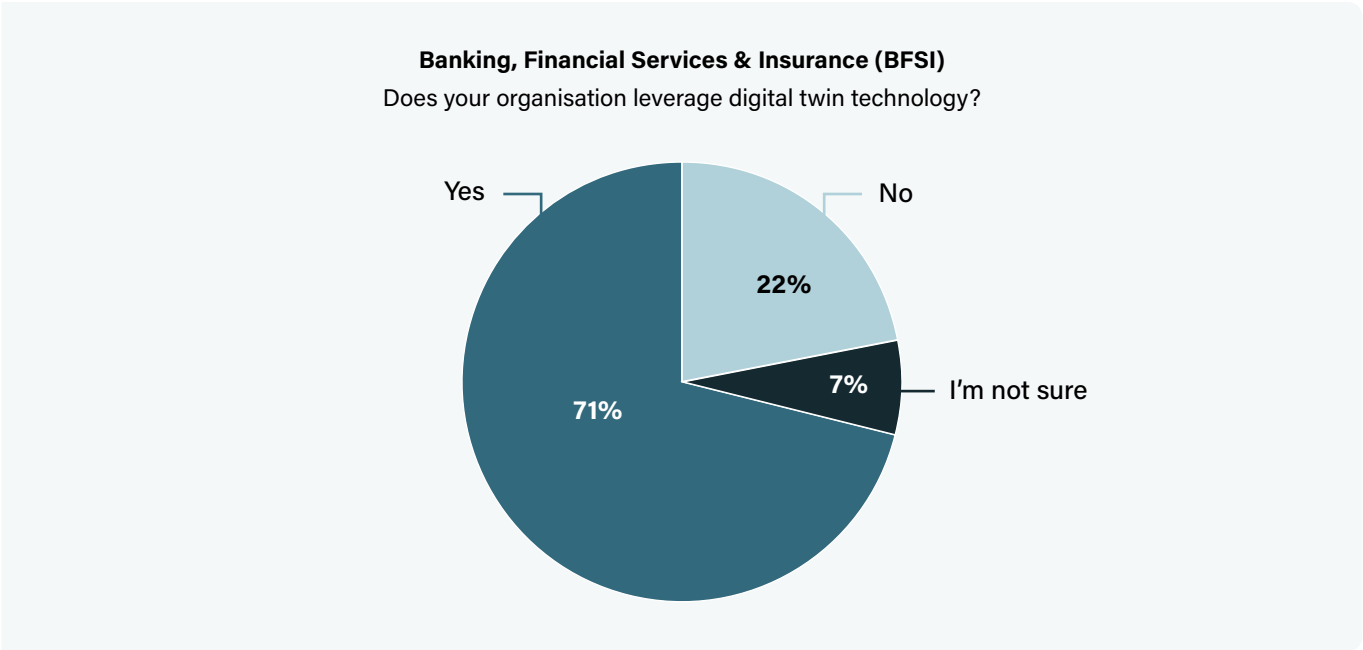
Digital twinning is not a totally new concept. In fact, according to a survey by Altair, 71% of respondents in the banking, financial services and insurance (BFSI) sector stated that their organisation already uses digital twin technology (see **Figure 3**). Also, 64% stated they are ‘highly knowledgeable’ about digital twin solutions.

A digital twin can be used to quantify the macro impacts of system changes, such as financial stability. The technology can also be used in stress testing to ensure the safe functioning of the system under bespoke scenarios, and to evaluate the extent to which changing the parameters of system features and design can reduce risk and / or optimise performance.

While simulations and digital twins both use digital models to replicate products and processes, there are some key differences between the two. Digital twins are arguably better from a quality standpoint. Simulations are run in virtual environments that may be representations of a physical environment, but do not integrate real-time data, and theoretical data parameters are set before the simulation is run. In contrast, digital twins use AI and automation to integrate real-time data and create an exact virtual representation of a process, updating in line with adjustable data inputs.

Figure 3: Financial Sector Firms and Their Use of Digital Twin Technology in 2023

Source: Altair Survey Report¹²



¹² Altair Engineering. (2023). 2023 Global Digital Twin Survey Report Vertical Breakdown: Banking, Financial Services, and Insurance. [Online]. Altair. Last Updated: 2023. Available at: https://altair.com/docs/default-source/resource-library/altair_survey-report_bfsi.pdf?sfvrsn=6fa8a1c [Accessed 22 November 2023].

Taking a Digital Twin Approach to Address Operational Resilience Challenges

Digital twins help financial firms to address DORA and UK operational resilience challenges on four fronts; resources, data, technology and third-party risk.

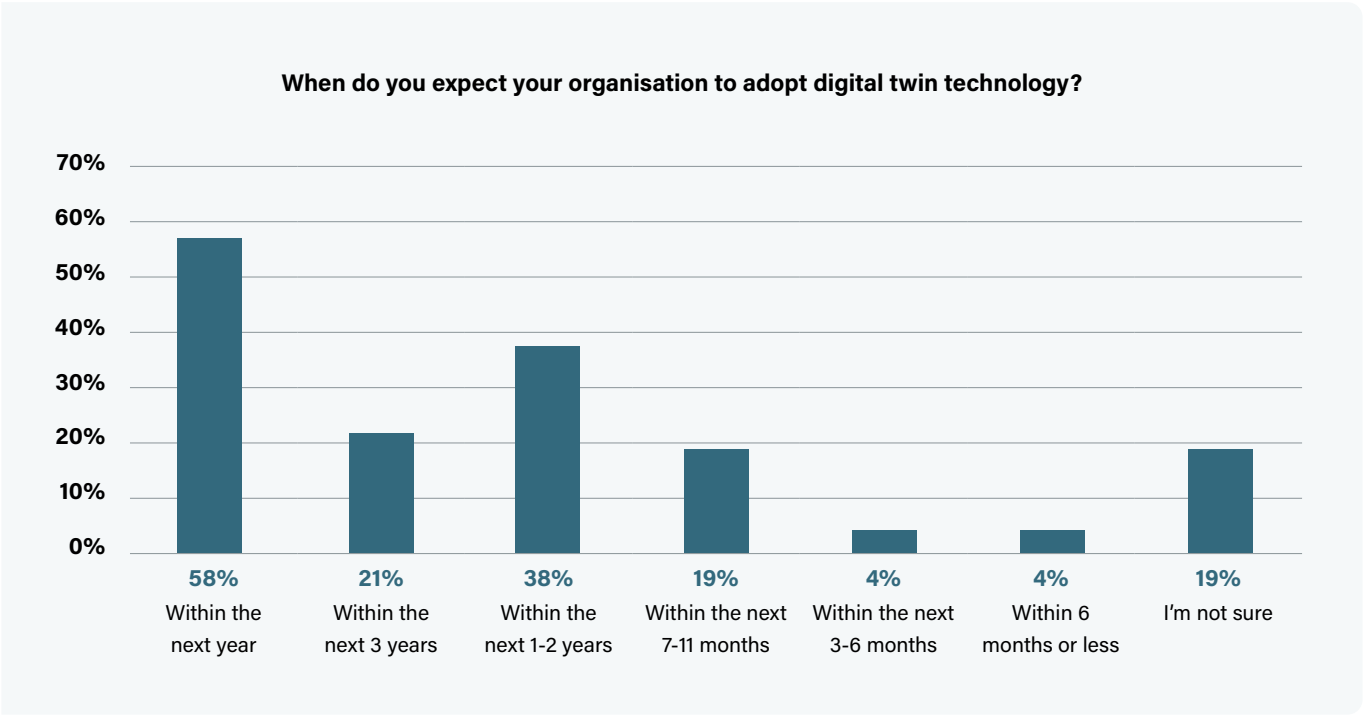
- 1. Resource Constraints:** Testing is commonly undertaken out-of-hours because production environments cannot perform their essential daily functions and be tested at the same time. Typically, financial institutions address scenario testing requirements by employing more staff (i.e. testing teams) in the hope of speeding up the testing process. This results in increased staffing costs and can lead to 'analysis-paralysis' and divert attention from core business practices. Digital twins co-exist with the production environment and require minimal human intervention thanks to the incorporation of automation / ML, which can also mean that the speed and frequency at which certain scenarios can be tested is increased.
- 2. Data Silos:** A typical data challenge that firms face is the lack of sufficient data to test the various scenarios, as well as the limitations of a human test designer to create a sufficiently wide variety of scenarios to test the potential impact of unforeseen events. The use of cleansed, plausible real-world data in the digital twin model eliminates the effort associated with the cleansing and validation of data specifically for testing in the simulation approach. In addition, digital twins can break down data silos across different functions (e.g. across Business, IT, Security and Risk teams and across teams in different geographies) and unlock value across the product life cycle, because it aggregates historical data and real-time data in one place. This encourages a cohesive, universal data management framework, engendering a more holistic, simplified data view of the firm.
- 3. System Vulnerability:** Banks and other financial institutions are constantly under threat from costly and damaging cyber-attacks. The dynamic view of systems and processes facilitated by the digital twin can enable organisations to detect potential security threats in real-time and take timely action to protect their customers and assets. In addition, it allows businesses to gain greater insight into their operations without having to invest heavily in infrastructure upgrades or additional personnel resources, while also reducing future system downtime in the case of an unforeseen event.
- 4. Third-Party Risks:** Given that the operational resilience regulatory landscape is still evolving, it is critical that financial firms utilise an agile, configurable platform that can support dynamic real-time data inputs and allow them to meet new requirements as they arise. Achieving regulatory compliance for testing can be challenging due to the reliance of financial firms on third-party systems. In particular, oversight of third-party providers is important to ensure that any contracts between financial firms and third-party providers are compliant under the terms of DORA. For example, financial firms must inform the supervisory authorities of any ICT services that support critical or important functions and that due diligence of third-party services has been conducted.^{13,14} Third-party vendors are not always willing to provide critical information to their financial firm clients, or participate in the scenario testing that financial firms are mandated to do because the vendors have little incentive to do so. In deploying a digital twin, banks have something to entice third-party ICT service providers. Many vendors only sell a single product into a bank, whereas the bank will have numerous third-party products embedded into their IT landscape across the enterprise. To create the digital-twin, all third-party vendors are included, and banks can allow the third-parties to see how their solution interacts with the other platforms that the bank has. This information can be very advantageous to third-party vendors to use in their own testing phases, meaning they will be more willing to work with the bank in its third-party risk assessment.

¹³ ICT services refers to the application of business and technical expertise to enable organisations in the creation, management, and optimisation of/access to information and business processes. These include cloud services and network security solutions. Techknowledgey. (2018). *Examples of IT Services*. [Online]. <https://www.techknowledgeyinc.com/7-examples-of-it-services/>. Last Updated: 15 November 2018. Available at: <https://www.techknowledgeyinc.com/7-examples-of-it-services/> [Accessed 27 November 2023].

¹⁴ Elteste, U and Nietsch, T. (2023). *EXPLORING DORA: EU TIGHTENS IT SECURITY RULES FOR THE FINANCIAL SECTOR, TARGETING "CRITICAL" THIRD-PARTY PROVIDERS*. [Online]. K&L Gates. Last Updated: 13 January 2023. Available at: <https://www.klgates.com/Exploring-DORA-EU-Tightens-IT-Security-Rules-for-the-Financial-Sector-Target> [Accessed 22 November 2023]

Interestingly, while the Altair survey revealed that of the respondents who stated that they do not currently leverage digital twin technology, just 4% expect their organisation to adopt it within the next six months (see **Figure 4**). This is an intriguing finding, given that most organisations that use digital twins say it is very important to their operations. As operational resilience regulatory pressure grows, financial firms that do not utilise digital twin capability will find themselves unable to comply robustly with the operational resilience regulatory mandates.

Figure 4: Digital Twin Implementation Horizon for BFSIs that do not Currently use Digital Twin Technology
Source: Altair¹⁵



¹⁵ Altair Engineering. (2023). *Examining the Data on Digital Twin in the Banking, Financial Services, and Insurance Industry*. [Online]. Altair Engineering. Last Updated: 11 August 2023. Available at: <https://altair.com/newsroom/articles/examining-the-data-on-digital-twin-in-the-banking-financial-ser> [Accessed 22 November 2023].

Challenges of a Digital Twin Implementation

The digital twin approach is heavily reliant on the accuracy of the data it utilises. If incorrect or old data is used in the digital twin model, it will produce unreliable results, potentially leaving the financial firms’ systems vulnerable to risks that will not be properly addressed or mitigated. Ultimately, successful digital twin implementation depends on capturing specific parameters that eventually help calibrate performance and design improvements, and this is impossible without high-quality, real-time data. Data preparation is often extremely time consuming, however, because it has to be gathered from data silos with different business departments and cleansed, validated and wrangled into a usable format. Given the amount of effort needed to prepare the data, firms should consider outsourcing this process. If data is prepared in-house, the financial firm may not have the resources to process the broad and deep dataset required to create a digital twin model. Consequently from a quality control and resourcing standpoint, it is a challenge for financial firms to implement a digital twin model by themselves.

Additionally, although digital twins can help identify cyber / security threats, they can themselves still be susceptible to a security breach if not carefully overseen. Bad actors could create an almost identical yet inconspicuous model of the digital twin, insert it into a production environment in order to inject malware into the ecosystem or steal data.

Solutions to Overcome Challenges of Creating and Using a Digital Twin

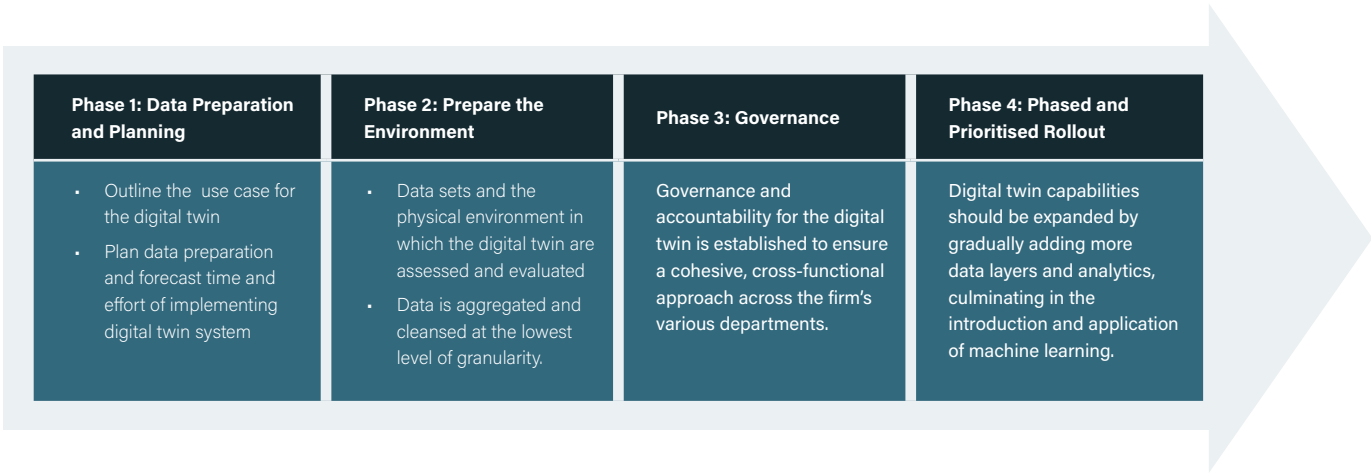
The successful implementation of a digital twin model requires firms to have already created a well-defined data strategy plan tailored to their firm’s unique specifications. **Figure 5** depicts a model digital twin data strategy plan.

Given that digital twins consist of highly sophisticated hardware and software, the development, implementation and maintenance of a digital twin is typically highly complex. During the initial phase – digital twin data strategy – the firm may reach out to reputable, compliant third party subject matter experts with experience of implementing digital twin models. Failure to properly execute a digital twin model can lead to an unnecessary strain on resources and higher implementation and running costs, while leaving the firm vulnerable to operational risks. In many ways, poorly implementing a digital twin framework may do more harm than not implementing one at all.

Crucially, failure to develop a robust and agile digital twin model could mean that financial firms will fail to achieve operational resiliency compliance – especially as existing regulatory frameworks, such as DORA, continue to evolve and become more nuanced. The importance of successfully implementing a digital twin framework cannot be downplayed.

Figure 5: Digital Twin Data Strategy Plan

Source: Nvidia¹⁶, GreySpark analysis



¹⁶ Nvidia. (2023). *5 Steps to Get Started with Digital Twins*. [Online]. Nvidia. Last Updated: January 2023. Available at: <https://resources.nvidia.com/en-us-omniverse-industrial-digital-twins/omniverse-enterprise-5-steps> [Accessed 22 November 2023].

Revolutionising Scenario Testing

The digital twin is increasingly becoming an integral part of financial firms' operational resilience frameworks. According to MarketsandMarkets, digital twin technology in the financial services sector is set to be worth USD 0.5 billion by 2028.¹⁷

Increasing the robustness of the operational resilience in the financial sector has undoubtedly become one of the top priorities for regulators this decade, resulting in regulatory frameworks such as DORA and the UK's BoE, PRA and FCA Operational Resilience. However, these requirements have ultimately exposed inadequacies and rigidities in existing scenario testing systems, especially from a resource and data standpoint, putting firms at risk of not only future operational disruption, but also of regulatory retribution.

A digital twin helps to address these challenges for in-scope firms by providing a flexible, universal and entirely realistic scenario testing framework, representing an exciting new frontier for firms seeking to gain greater insight into their operations, and crucially, maintain regulatory compliance.

¹⁷ MarketsandMarkets. (2023). *Digital Twin in Finance Markets*. [Online]. MarketsandMarkets. Last Updated: April 2023. Available at: <https://www.marketsandmarkets.com/Market-Reports/digital-twin-in-finance-market-54154446.html> [Accessed 22 November 2023].