CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

Dynamic Scenario Library

2025 EDITION

VERSION 1.0 | SEPTEMBER 2025 | TLP CLEAR

Contents

1 Background & Aims

In September 2023, following a preliminary discussion paper, members of the Operational Resilience Collaboration Group (ORCG), under the auspices of the Cross Market Operational Resilience Group (CMORG), agreed to develop a sectoral facility for community-agreed scenarios known as the **Dynamic Scenario Library** (DSL) for initial publication in 2024.

Aims

The DSL is designed to be a shared resource which contains a catalogue of categorised and individually described scenarios, constructed using a common design methodology. It aims to:

1. Provide a library of detailed scenarios, reflective of the current threat and risk landscape, that individual firms, authorities, and the sector can leverage and customise for the purposes of scenario planning and exercising.
2. Enable greater levels of consistency across the sector through the collective use of a commonly agreed Library of base level scenarios.
3. Increase understanding regarding the impact of the scenarios contained within the strategic risk register, in order to support appropriate mitigation activity.

NB: The DSL is designed to be a sector resource to support firms in their operational resilience scenario testing. It does not represent a minimum set of scenarios that firms are expected to test against or to remain within Impact Tolerance (ITOL). Conversely, nor does testing against each scenario confer compliance with regulation. Which scenarios, if any, used and how they are adapted is for individual firms to decide.

2 Operating Model

Interactions with other CMORG capabilities

To achieve its aim of providing a set of scenarios that reflect the current threat and risk landscape, the DSL is informed by two key CMORG Capabilities (see Figure 1):

A) Threat Monitoring: which provides a periodic mechanism for the pooling of threat related information from across the sector. Should an emerging or changing threat dictate, an additional ad hoc threat monitoring process provides the means to provide timely updates with changes then made, where appropriate to the Strategic Risk Register and DSL.

B) The CMORG Strategic Risk Register (SRR); the SRR provides an industry-agreed view on the most critical threats to the financial sector. It is intended to provide strategic direction to the CMORG collective action programme, including informing the prioritisation of thematic focus areas, outcomes and resourcing. As an input into the DSL, it will inform scenario inclusion, prioritisation of their production, and maintenance.

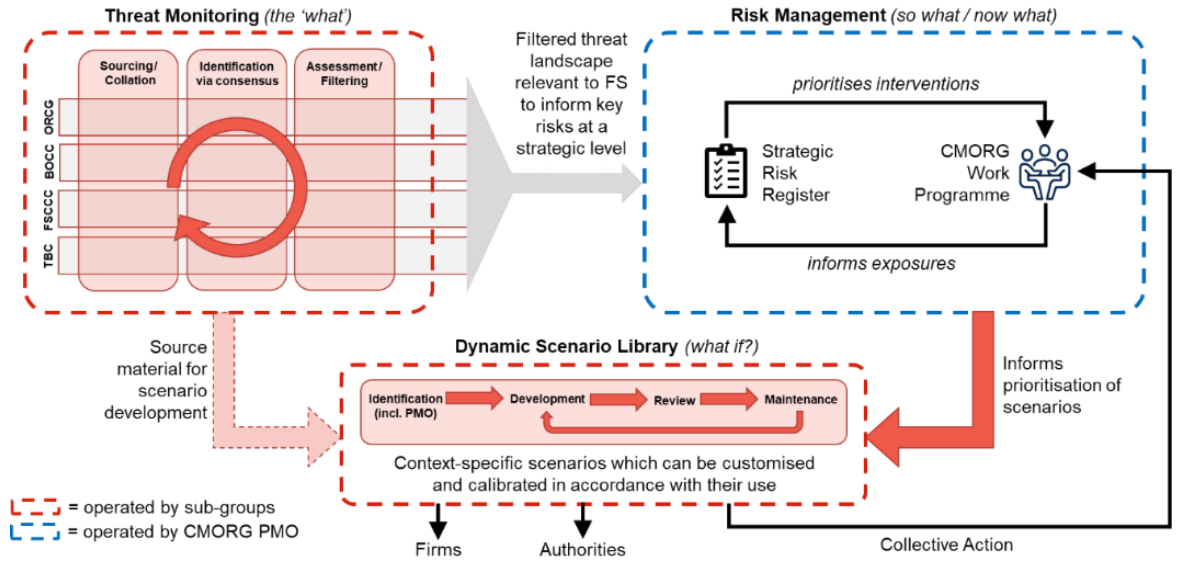

Figure 1: Dynamic Scenario Library in context of Threat Monitoring and the Strategic Risk Register

Figure 2 describes how these capabilities work together with the DSL in the event of a new or rapidly changing threat to the UK Financial Sector. In this example, the deteriorating geo-political environment and suspicious marine activity lead to a change in threat assessment (1), leading to a new entry in the CMORG SRR (2) and requests a more detailed risk review to better understand the extent to which the financial sector may be exposed. In parallel with an assessment of potential impacts under reasonable worst-case conditions, CMORG commissions the development of a linked scenario (3) for inclusion within the DSL.

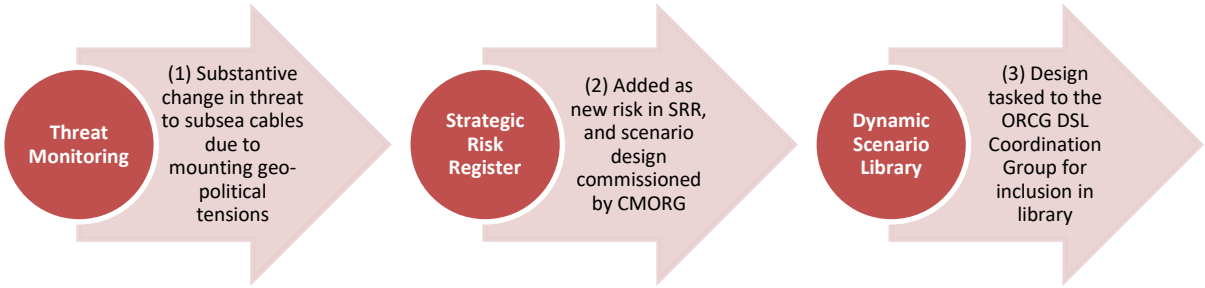

Figure 2: Workflow for worked example (subsea cables)

Note: Although ORCG own the scenarios within the DSL, any member of CMORG can also propose changes to the ORCG outside of Threat Monitoring or the SRR driven process. This can either be done directly to the ORCG or via CMORG PMO if needed. Requests will then be triaged by the ORCG DSL Coordination Group against the scheduled updates and then actioned in line with the scenario library lifecycle outlined below.

Scenario Library Lifecycle

The lifecycle for running the library includes the following phases:

- **Identification**: The ORCG DSL Coordination Group (DSL CG) performs an evaluation of potential new or changed scenarios (including removals), informed by threat landscape and SRR priorities, combined with any backlog of scenario requests which have been received since the previous library refresh.
- **Review**: Once potential scenario additions/changes/removals have been identified, the relevant CMROG subgroups are consulted, after which development is assigned to an ORCG member firm(s) to action.
- **Syndication**: All scenario updates are circulated to relevant CMORG subgroups for feedback ahead of approval by the ORCG.
- **Distribution**: Finally, the CMORG PMO sends revised library to CMORG ahead of external publication.

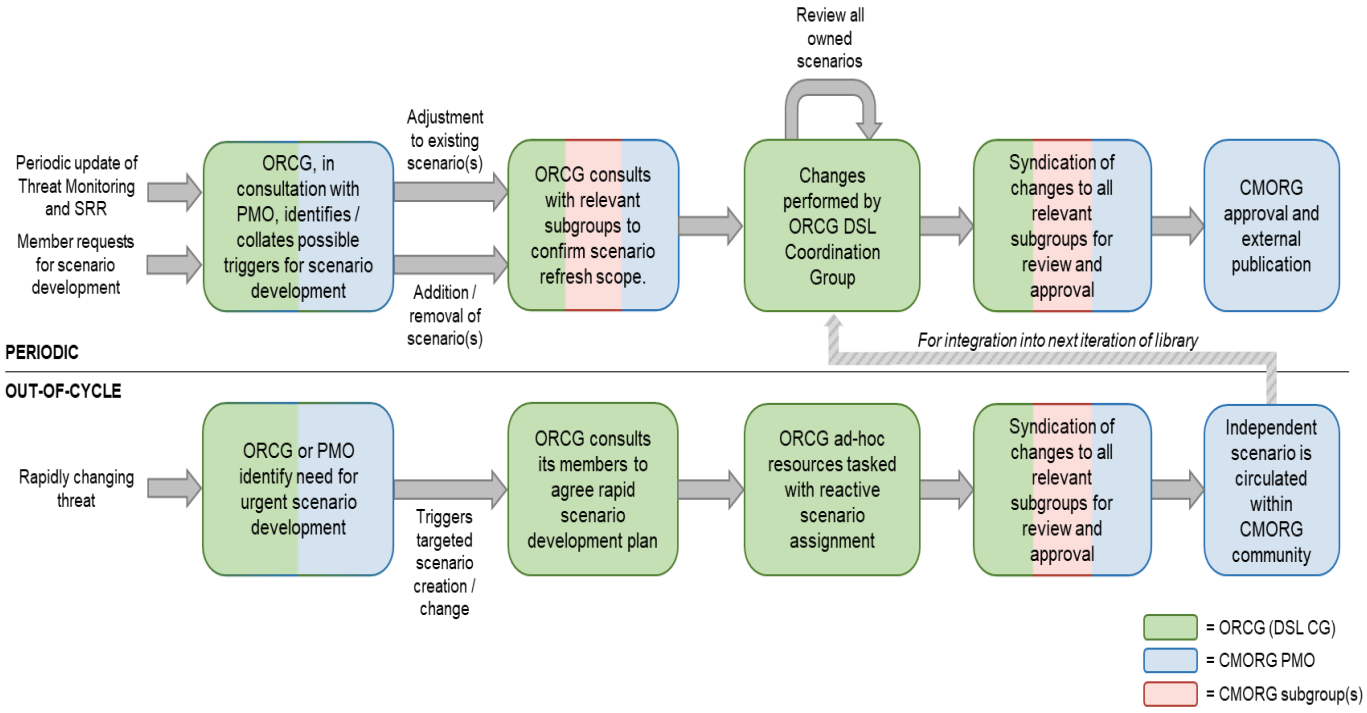

Figure 3: Scenario Library Lifecycle Workflow

DSL Roles & Responsibilities: RACI Model

Accountability for the DSL lies with the ORCG, with the DSL Coordination Group (a standing sub-group of the ORCG) responsible for its operation on behalf of the ORCG. The DSL CG will be supported by the CMORG PMO, as required, with the coordination across CMORG subgroups and with the interlock with key inputs into the DSL such as the Strategic Risk Register (SRR). CMORG PMO will also ensure CMORG are advised of any relevant status updates or items for escalation.

The underlying DSL methodology is owned and maintained by ORCG, in consultation with other relevant subgroups. ORCG are responsible for the selection (and de-selection), creation and maintenance of the scenarios within the library; with technical subgroups consulted for scenarios that related to their respective specialism. A separate ad hoc process for urgent out-of-cycle scenario development requests is also available.

Ref	Task	Description	ORCG	ORCG DSL CG	Relevant CMRG Subgroup	CMORG PMO	CMORG
1	**Coordination of the Dynamic Scenario Library**	Collection point for any trigger events which may instigate library update and to coordinate with relevant parties	A	R			
2	**Maintenance of the Dynamic Scenario Library**	(see below)					
2.1	Maintenance of the Dynamic Scenario Library methodology	Periodic review and adjustment of the methodology to ensure it remains fit for purpose and meets industry expectations	A	R		I	
2.2	Deciding to add new or remove existing scenario (as part of periodic review cycle)	Additions or removals requested by CMORG (via PMO) to the existing scenario library catalogue following updates to the Strategic Risk Register and/or by subgroup request	A	R	C	C	
2.3	Deciding to add new scenario (out of cycle)	Urgent need for new scenario development based on rapidly emergent risk to the UK Financial Sector	A	R	C	C	
2.4	Updating an existing scenario	Adjusting existing scenarios in line with changing threat landscape	A	R		C	
2.5	Review and approve changes (including additions/removals) to the library	Relevant subgroups consulted on changes to the Dynamic Scenario Library, and provide subgroup level sign-off	A	R	C	C	
3	**Publication of the Dynamic Scenario Library**	Distribution of the published DSL	C			R	A

Notes:

- A = Accountable; R = Responsible; C = Consulted; I = Informed
- Maintenance of the DSL methodology includes the annual review of this RACI model.
- The addition/removal of a scenario is a decision for ORCG in consultation with the relevant technical subgroup. If the scenario is linked to the SRR, then CMORG PMO should also be included.

3 How to use the Dynamic Scenario Library

Localisation / Customisation

A key design principle of the DSL is that firms can select and customise scenarios to their individual needs whilst still achieving a level of consistency across firms in the terms of the base scenario.

As such, when using the library, firms are encouraged to make the changes required to ensure relevance to their business. Each firm will have differences in the market(s) and geographies they operate in, and the manner in which services are delivered. All these factors will determine the relevance of either the scenario itself and/or different aspects of the scenario.

The primary means of localisation/customisation are the 'stress variables' which can be used either as an 'options list' for increasing the severity of the base scenario or for the different stages within a stress test scenario format where the variables are used to 'ratchet up' the severity of a scenario from its 'base scenario' in order to identify the point in which impact tolerance would be breached. Each scenario in the DSL contains between 3 and 5 scenario variable categories and levels of severity. Although options are provided, firms can use and alter as required.

Scenario Causation to Impact Mapping

In addition to the 'stress variables' outlined in each scenario, please also refer to Annex B 'Scenario Causation to Impact Mapping' which can be used to scale the impact by moving along the impact options based on the scenario cause. For example, there are three cloud related impacts described under the Technology resource pillar; 1) the loss of an availability zone; 2) the loss of a cloud region; 3) the global loss of cloud service provider services, e.g. a relational DBMS. Firms have the option to adapt the scenario they are playing to reflect their testing needs.

It is recommended that any changes made to the base scenario are kept captured in the suggested table at the bottom of the scenario (or equivalent) to aid traceability with regard to the scenario storyline and calibration.

Case Studies

Likewise, case studies have been added to support the assessment of plausibility in addition to the scenarios being selected for inclusion in the library based on the Strategic Risk Register. Firms are encouraged to identify and use the most relevant case studies to their firm's business and operations.

Although some case studies include links to sources and/or reference material, where citing any case studies from the DSL, it is the responsibility of the firm doing so to validate any numbers/statements included within them.

For further information regard the layout and expected content within a scenario (see Annex A).

Compound Scenarios

The DSL contains scenarios based on an agreed set of causal events with the aim of achieving coverage over the principal types of disruption (see Annex B). However, incidents are often multifaceted in nature and rarely neatly conform to a single causation type. For example:

- a technology hardware failure could be exacerbated by human error in recovery; or

- the simultaneous unavailability of technology and key third party who share a dependency with a firm on a common third-party technology supplier; or
- a denial of access to a building from a localised incident whilst experiencing a disruption to remote access infrastructure, impacting the ability to leverage home working as a recovery strategy.

As such there are more permutations of any given scenario or combination of scenarios than can be catered for in the DSL. Therefore, firms should consider how aspects of the different scenarios within the DSL can be combined to reflect a particular risk deemed relevant to test against. Compounding scenarios may also offer firms the opportunity to explore multiple facets of their response and recovery capabilities more efficiently through a lower volume of test events.

Feedback

All users of the DSL are encouraged to feedback observations to ORCG on the utility of the scenario used, which will then be fed into future iterations as part of a continuous improvement cycle.

Supporting guidance

This document should be read in conjunction with the *CMORG Guidance for Firm Operational Resilience*[1], in particular Section 5.3 'Scenario Themes', which contains scenario themes that are impact-based and cause agnostic to help inform scenario planning and testing. The relationship between the scenario themes and scenarios in this library are covered in the Annex B. It is envisaged that the DSL may supersede the example scenarios in the CMORG Guidance as part of a future refresh.

[1] Guidance for Firm Operational Resilience - TLP Clear - CMORG.pdf

4 DSL Scenario Library Index

The scenarios contained with the DSL are outlined below with the corresponding SRR reference, Scenario Owner and when the scenario was published.

Category	Ref	DSL Scenario (Causation)	SRR	Dom	SRR L1 and L2 Alignment / Comments	Consulted	Last Published
1. Technology & Data (Cyber)	1.1	Cyber Attack - Malware e.g. Ransomware	Yes	3	L1 - Ransomware and malicious exfiltration of data/data deletion/corruption. Covers SRR Scenario 3.1. and 3.2.	CCG	MAR25
	1.2	Cyber Attack – Multiple firms targeted through supply chain attack	TBC	TBC	TBC	CCG	MAR25
	1.3	Generative AI Compromise of Authentication (Staff Account Creation)	No	N/A	N/A	CCG & CIOF	JUN25
	1.4	Generative AI Compromise of Authentication (Customer Account Creation)	No	N/A	N/A	CCG & CIOF	JUN25
2. Technology & Data (non-cyber)	2.1	Poorly Executed Change	No	N/A	SRR does not include 'poorly executed change' however SRR Scenario 9.1 explores *the failure of a firms' IT technology infrastructure, controls and processes that results in systemic impacts to the wider sector.*	CIOF	MAR25
	2.2	Hardware/ Software Failure	Yes	9	L1 - Failure of operational resilience due to failure of obsolete IT infrastructure. SRR Scenario 9.1.	CIOF	-
	2.3	Procedure/ Human Error	No	N/A	N/A	CIOF	-
3. Physical Security	3.1	Terrorism - Mass Destruction	No	N/A	N/A	ORCG	MAR25
	3.2	Terrorism - Marauding Armed Intruders	No	N/A	N/A	ORCG	MAR25
	3.3	CBRN Attacks	No	N/A	N/A	ORCG	-
	3.4	Civil Unrest	No	N/A	N/A	ORCG	MAR25
4. Geopolitical	4.1	Intrastate Conflict	No	N/A	N/A	ORCG	-
	4.2	Regional Conflict	Yes	13	L1 - Geopolitical tensions rising to cause detrimental harm to UK sovereignty through nation-state threat actors to significant inter-	ORCG	-

Category	Ref	DSL Scenario (Causation)	SRR	Dom	SRR L1 and L2 Alignment / Comments	Consulted	Last Published
					state conflict. SRR Scenario 13.2.		
	4.3	Disruption to Undersea Cables	Yes	13	L1 - Geopolitical tensions rising to cause detrimental harm to UK sovereignty through nation-state threat actors to significant inter-state conflict. SRR Scenario 13.1 Undersea Cables.	ORCG	MAR25
5. Industrial Accidents	5.1	Major Industrial Accidents (Nuclear)	No	N/A	N/A	ORCG	-
	5.2	Major Industrial Accidents (Non-Nuclear)	No	N/A	N/A	ORCG	-
6. Natural Hazards & Public Health	6.1	Severe Weather (e.g. Hurricanes/ Tropical Storms)	Yes	12	L1 - Loss of Business Process Outsourcing or other operations due to climate change	ORCG	MAR25
	6.2	Non-weather geo-hazards (e.g. Earthquake)	No	N/A	N/A	ORCG	-
	6.3	Severe Contagious Disease e.g. Pandemic	Yes	4	L1 - Pandemic influenza or communicable disease. SRR Scenario 4.1.	ORCG	MAR25
	6.4	Severe Space Weather	No	N/A	N/A	ORCG	MAR25
7. Critical National Infra	7.1	Localised Loss of Power	Yes	2	L1 - Failure of energy supply due to prolonged outage on the National Grid	ORCG	MAR25
	7.2	National Power Outage (NPO)	Yes	2	L1 - Failure of energy supply due to prolonged outage on the National Grid	SEG	MAR25
	7.3	Loss of Telecoms / Network Infrastructure	Yes	1	L1 - Telecommunications failures (fixed and mobile telephone services, and broadband). SRR Scenario 1.1	CIOF	-
8. Third Party	8.1	Loss of Material Third Party (Inc. CSP)	Yes	5 & 7	L1 - Loss of, or disruption to, a TP or critical supplier. SRR Scenario 5.1 L1 - Severe impact to the ability of a cloud services provider to continue to provide services to its clients. SRR Scenario 7.1	TPRG	MAR25
	8.2	Loss of an FMI	Yes	6	L1 The disruption to, or complete failure of, core payment systems infrastructure. SRR Scenarios 6.1 and 6.2.	TPRG	MAR25

Category	Ref	DSL Scenario (Causation)	SRR	Dom	SRR L1 and L2 Alignment / Comments	Consulted	Last Published
	8.3	Loss of a G-SIB or G-SFI	Yes	5	Loss of, or disruption to, a third party or critical supplier, including a G-SIB or G-SIFI. SRR Scenario 5.1.	SEG	-

5 The Dynamic Scenario Library

Technology & Data (Cyber)

Cyber Attack – Malware (Ransomware)	**Scenario Category**
	Technology & Data (Cyber)

Scenario Description						
Overview	This Scenario explores a sophisticated double extortion ransomware attack, resulting in the exfiltration of internal [firm] data and the encryption of core IT Infrastructure, applications and end point devices, causing Important Business Services (IBS) to be disrupted.					
Cause	The threat actor exploits an unpatched server to successfully deploy malware which encrypts servers [*some platforms such as MS Windows are viewed as higher risk than other*] supporting core infrastructure and IT applications as well as colleague's end-point devices.					
Impact (Incl. Scale)	• The threat actor moves through the network – compromising privileged accounts, domain controllers and backups. The threat actor also exfiltrates customer PII. • The attack renders all impacted devices unusable causing significant disruption to internal and external technology services. Response capabilities are also limited as colleagues cannot access their devices. • Although the scenario assumes that preventative mechanisms have been bypassed the disruption has been contained to a [single] Active Directory domain and has impacted [50%] of the Windows servers rendered the Active Directory inoperable. • The attack targeted servers but [25%] of user devices have also been encrypted across the entire estate, impacting all staff supporting IBS in addition to those IBS reliant on impacted servers. • In addition, there are impacts to resources used to recover services (backups, code stores) and support business response e.g. impact to systems required to execute continuity strategies. • The threat actor posts [firm] as the victim on their attack, demanding a $[xx] million ransom to release the systems and return customer PII data. • Media spreads the news, and [firm] faces pressure to comment. • Other Financial Services firms confirm they have executed disconnection protocols and will only reconnect once they are comfortable it is safe to do so. • Within [3 days], the ransomware threat actors begin leaking PII as a pressure tactic. • The cyber response playbook has been invoked.					
[Risk] Coverage	People ☐	Property ☐	Technology ☒	Data (Availability) ☒	Data (Integrity) ☒	Third Party ☐
Characteristics	• **Rapid onset** - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place. • **Low predictability/highly changeable -** Threat Actor adapts to counter moves. • **High persistence** - potential for recurring periods of disruption. • **Uncertain duration** - of investigation, containment and recovery time makes estimating business recovery times difficult. • **Information asymmetry** - key information regarding the incident may not be fully visible.					

	• **Disrupted Communication** - Internal and external communication channels are impaired by the nature of the incident. • **Higher scrutiny** and potential to undermine stakeholder trust - through perceived or actual lack of action/transparency due to nature of incident.
Assumptions	• Incident happens on a peak and/or significant trading day with above average volume (in line with the worst-case scenario used for setting impact tolerance). • Threat actor is capable and sophisticated deploying ransomware as a business, as such both primary and backups have been encrypted. • On completion of the Technical Recovery an application recovery/rebuild will be required followed by data and business reconciliation.

Stress variables *(illustrative levels, to be adjusted as appropriate)*					
# platforms impacted	Windows ☐	Linux ☐	Midrange ☐	Mainframe ☐	Other ☐
Servers Impacted	60% ☐	70% ☐	80% ☐	90% ☐	100% ☐
End points impacted	30% ☐	40% ☐	50% ☐	50-75% ☐	<75% ☐

Case Study	
Causation/ Impact (Risk Coverage):	On 27 June 2017, the container shipping company Maersk, was one of a number of organisations, across a range of countries, that were the victims of the NonPetya cyber-attack which resulted in widespread encryption and unavailability of technology and data.
Impact (scale):	The attack spread across Maersk network crippling it within 7 minutes. 45,000 PCs and 4,000 servers were infected impacting 76 global port terminals which had to shut down. Maersk was forced to return to manual operation and handle backlog in orders. The attack was estimated to cost the organisation $300m.[2]
Duration:	Using manual operations, it was 2 days before Maersk could take orders from existing customers and 6-12 days before terminals gradually progressed to more normal operations. Operations didn't return fully to normal until mid-July.
Compound Scenario Considerations:	As threat actors will often be opportunistic in the timing of their attacks, cyber scenarios can be combined with a range of other scenario causations. For example, the rapid shift to homeworking in response to the COVID-19 pandemic created a much large attack surface during a time when firms had an even greater reliance on technology to maintain critical services.
Takeaways:	The attack on Maersk demonstrated the vast disruptive potential of ransomware and speed of onset. It highlighted the importance of network segmentation, patch management and backups being isolated. These types of attack are also a reminder that communications systems, key in any incident, may also be impacted and the plans and tools required to recover need to be accessible without dependence on the availability of the technology that may be impacted.

[2] LRQA. NotPetya ransomware attack on Maersk – key learnings. Available [Online]: Notpetya ransomware attack on Maersk - key learnings | LRQA

Cyber Attack – Multiple firms targeted through supply chain attack	**Scenario Category**
	Technology & Data (Cyber)

Scenario Description						
Overview	This scenario explores a sophisticated supply chain attack at a software provider, resulting in compromised software being delivered to customers (including Financial Services firms), which enables compromise of the customer's system(s). This impacts Important Business Services (IBS) in multiple Financial Services firms.					
Cause	The threat actor infiltrates a software provider and deploys malicious code to compromise a software product that is commonly used in supporting core IT systems. The compromised software is then delivered to customers through the trusted software provider, with the customer accepting the software by default, installing the compromised software version to core IT systems that support IBSs.					
Impact (Incl. Scale)	• Unusual traffic is detected in core IT systems, but the root cause cannot be identified immediately. • Some individual firms decide to take their potentially compromised systems offline and perform investigation, resulting multiple IBS disruption. • Services remain unavailable at end of day and investigations remain ongoing with no estimated time of when services will be resumed. • Multiple firms identify unusual traffic in core IT systems following a recent update of a commonly used software from the same software provider. • The compromised software provider is a leading software company and hence there is a risk of broad impact to the market as multiple Financial Institutions are impacted. • Software fix from the vendor is not made available until Day 2 of the incident. • The is widespread media coverage reflecting the number of firms impacted and the nature of the outage. • The cyber response playbook has been invoked.					
[Risk] Coverage	People ☒	Property ☐	Technology ☒	Data (Availability) ☒	Data (Integrity) ☒	Third Party ☒
Characteristics	• **Rapid onset** - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place. • **Low predictability/highly changeable** - Threat Actor adapts to counter moves. • **High persistence** - potential for recurring periods of disruption. • **Uncertain duration** - of investigation, containment and recovery time makes estimating business recovery times difficult. • **Information asymmetry** - key information regarding the incident may not be fully visible. • **Disrupted Communication** - Internal and external communication channels are impaired by the nature of the incident. • **Higher scrutiny** and potential to undermine stakeholder trust - through perceived or actual lack of action/transparency due to nature of incident.					

Assumptions	• Incident happens on a peak and/or significant trading day with above average volume. • Compromised software is a commonly used products across firms. • Highly capable threat actor and sophisticated supply chain attack. • On completion of the Technical Recovery an application recovery/rebuild will be required followed by data and business reconciliation.				
Stress variables *(illustrative levels, to be adjusted as appropriate)*					
# platforms impacted	Windows ☐	Linux ☐	Midrange ☐	Mainframe ☐	Other ☐
Servers Impacted	60% ☐	70% ☐	80% ☐	90% ☐	100% ☐
End points impacted	30% ☐	40% ☐	50% ☐	50-75% ☐	<75% ☐
Case Study					
Causation/ Impact (Risk Coverage):	On 13 December 2020, FireEye, Microsoft and SolarWinds released a statement relating to an ongoing global intrusion campaign that involved a supply chain intrusion vector leveraged by an automatic update mechanism in the SolarWinds Orion IT management software. The hacked code created a backdoor into 18,000 customers' IT systems when they installed routine software updates. This potentially enabled threat actors to install further malware to infiltrate those infected organisations.				
Impact (scale):	The Orion software system is used by 33,000 companies to manage IT resources, including Fortune 500 companies and multiple agencies in the US government.				
Duration:	News of the attack was released in December 2020, by which time threat actors had potentially had access to exposed organisations for several weeks. Initial updates to address the vulnerability were released on 14 and 15 December.				
Compound Scenario Considerations:	The impact of this scenario could be exacerbated by news of a vulnerability being released a significant period of time before a fix is available, leaving organisations exposed to other threat actors seeking to capitalise on the vector.				
Takeaways:	Cyber-attacks on our suppliers can be as damaging as an attack on our own networks. Supply chain attacks, while not a new threat, are increasing in prevalence – and in the case of SolarWinds, where its scale was unprecedented, the force multiplier and domino effect of one well-placed attack had the potential to impact many others. Due consideration must therefore be given to ensure our third and nth parties are secure. Businesses are increasingly dependent upon third parties, including outsourced services, vendors, service providers, partners, and other financial institutions. It is important to assess the security risks of providing access to your data and services to third parties to demonstrate due care in your obligations to protect your organisation and customer data, while also minimising the potential for impacts to the wider system.				

Generative AI Compromise of Authentication (Staff Account Creation)	**Scenario Category**
	Other - AI

Scenario Description	
Overview	This scenario explores the use of Generative AI (Gen-AI) and Agentic AI by a threat actor to bypasses internal controls and create staff accounts. These accounts are then utilised at scale to conduct criminal activities e.g. data theft, unauthorised transactions and/or other forms of fraudulent action, before the impacted firm can identify and shut down the compromised accounts. Questions over the security and integrity of the impacted firm(s) systems result in some firms taking the decision to disconnect and customers withdrawing funds. Variation: In addition to bypassing internal controls, the threat actor was able to exploit a weakness in a commonly used verification tool. Other firms who use the same verification tooling begin to identify usual activity on their own networks, potentially undermining the integrity of the broader sector.

Cause	It has been discovered that an organised criminal group (OCG) has utilised novel techniques, leveraging Gen-AI and Agentic AI, to exploit existing staff identity and verification control within the firm and create fraudulent employee accounts. This includes:
	• The use of Gen-AI to create or manipulate documents to bypass background checks during the recruitment process.
	• Utilising open-source intelligence (OSINT) to search LinkedIn, company websites, data breaches (e.g. combolists), and dark web sources for employee templates, policies, or background check vendor details.
	• Utilising commercially available tools and open-source LLMs to create fake CVs with realistic job histories, cover letters matching job role language, performance reviews or academic references.
	• Bypassing Verification Controls:
	  ○ Voice clones for phone verifications: Using commercially available or open-source models to impersonate references during HR calls.
	  ○ Deepfake video calls: Deploying avatars or manipulated video using commercially available tools to pass 'live' video checks or remote onboarding interviews.
	  ○ Synthetic background data: Creating matching LinkedIn profiles, GitHub repos, or email history to satisfy due diligence checks.
	• Identification and Verification System Exploitation:
	  ○ Exploiting specific vulnerabilities, such as submitting synthetic identities against weak document/metadata checks.
	  ○ Using AI to script responses and bypass / crack poorly implemented authentication or identity federation systems.
	• Developing AI agents and an agentic workflow to automate the above processes, enabling the automation of reconnaissance, false account creation and maintenance, verification bypass and the generation of documents to enable abuse at scale. The use of agentic AI reduces the amount of effort from the attacker's perspective due to being objective based as opposed to requiring specific prompts to generate output.

Impact (Incl. Scale)	• Following an investigation into an unauthorised account creation, the firm has identified a vulnerability in a widely used identity verification tool. It is assessed that the vulnerability has existed for some time and enabled an attacker to create a fraudulent staff profile(s). • The firm is now unsure of the legitimacy of multiple staff members and is concerned about the data they might have collected, along with the scale at which other fake accounts could have been potentially created. • Other firms are then informed of the vulnerability with some firms taking the decision to disconnect from impacted firms until they are confident it is safe to reconnect. • Following broader investigations, it transpires that the verification tool is widely used across the sector and those firms using the tool beginning to identify similar activity raising the potential for a more systemic impact as firms pause certain activities whilst conducted their own cyber investigations. • During the investigation, law enforcement agencies have uncovered a pattern of blackmail and coercion attempts targeting staff at firms, where deepfake content has been used to pressure employees into completing fraudulent transactions or making unauthorised access requests with their credentials. • Leaks about the impact on some internal operations have spread on social media, causing widespread concern, reputational damage, and the possibility of a surge in withdrawals.					
[Risk] Coverage	People ☒	Property ☐	Technology ☒	Data (Availability) ☒	Data (Integrity) ☒	Third Party ☐
Characteristics	• **Rapid onset** - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place. • **Low predictability/highly changeable** - Threat Actor adapts to counter moves. • **High persistence** - potential for recurring periods of disruption. • **Information asymmetry** - key information regarding the incident may not be fully visible.					
Assumptions	• Incident happens on a peak and/or significant trading day with above average volume (in line with the worst-case scenario used for setting impact tolerance). • The OCG is a capable attacker with motive and means to act at scale. • Account reset options are likely to be highly complex and/or require significant manual intervention.					

Stress Variables				
Account impact	Customer ☐	Third Party ☐	- ☐	- ☐
Vulnerability age	3 Days ☐	1 Week ☐	2 Weeks ☐	1 – 3 Month ☐
Account Volumes	<10 ☐	<100 ☐	<1000 ☐	>1000 ☐
Identity Validation	Synchronous ☐	Asynchronous ☐	- ☐	- ☒

Other	An additional stress variable could consider material loan defaults or illegitimate market movements resulting from this attack, leading to wider market disruption and confidence impacts to the UK sector more broadly.
Case Study	
Causation/ Impact (Risk Coverage):	KnowBe4, a cyber security awareness training platform, recruited a software engineer for their internal AI team. When they sent the new hire their Mac workstation, it immediately started to load malware. Despite conducting four video conference-based interviews, background checks and standard pre-hiring checks, the hire was a fake IT worker from North Korea, who had used a valid but stolen US-based identity, that had been enhanced by AI. [3]
Impact (scale):	No breach occurred, and no customer data was accessed. The incident was contained quickly, but it revealed systemic vulnerabilities in hiring and vetting processes.
Duration:	The suspicious activity was detected within minutes of the laptop being activated. The operative was hired and onboarded over a short period, but the malware attempt occurred on the first day of device use (15 July 2024).
Compound Scenario Considerations:	The attacker used a Raspberry Pi, VPNs, and remote access from outside the U.S. to simulate working locally. The scheme involved multiple layers of deception: stolen identity, AI-generated photo, fake references, and plausible interview performance. The workstation was shipped to an "IT mule laptop farm", a tactic used to mask the attacker's true location.
Takeaways:	The attack on KnowBe4 highlighted the importance of having strong identification controls during hiring and IP monitoring for remote workers. These types of attacks could expose firms to loss of sensitive financial or customer data, and ransomware or sabotage attacks.

[3] blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

Generative AI Compromise of Identification Controls (Customer Account Creation)	**Scenario Category**
	Other - AI

Scenario Description	
Overview	This scenario explores the use of Generative AI (Gen-AI) and Agentic AI by threat actors to exploit weaknesses in controls to create customer accounts, exploiting a promotional period when higher levels of account creation were expected. These accounts are then utilised at scale to conduct criminal activities e.g. fraudulent transactions/withdraws, before the impacted firm can identify and shut down the compromised accounts. Questions over the legitimacy of customer accounts and the activities linked to them, and the security and integrity of the impacted firm more generally, result in some firms imposing additional controls and/or suspending activity with the impacted firm. Variation: In addition to bypassing internal controls, the threat actor was able to exploit a weakness in a commonly used verification tool. Other firms who use the same verification tooling begin to identify usual activity on their own networks, potentially undermining the integrity of the broader sector.

Cause	It has been discovered that an organised criminal group (OCG) has utilised novel techniques, leveraging Gen-AI and Agentic AI, to exploit existing identity and verification controls within the firm and create fraudulent customer accounts. The includes:
	• AI-generated identity bundles, combining fake names, addresses, NI numbers, and dates of birth in plausible formats using large language models (LLMs) and synthetic data generators (e.g. Faker libraries).
	• Generating realistic utility bills or bank statements using template-based document generators enhanced by Gen-AI to localise fonts, logos, and layout per institution (e.g. UK council tax bills).
	• The use of AI image models to erase spoof security features (e.g. holograms, microtext) from ID documents:
	  ○ Deepfake facial recognition bypass: Using AI-powered facial animation and deepfakes to simulate required head movements or expressions during live checks.
	  ○ Synthetic voice responses: Cloning voices for any required telephone authentication with AI services trained on small audio samples (like in-app 'verify your identity' calls).
	• Using LLM-guided form filling to automate bank account applications with tailored LLM responses based on known onboarding workflows.
	• The use of AI solvers for web CAPTCHAs, Route one-time passwords (OTPs) via SIM farms, or emulated devices to receive and forward two-factor authentication (2FA) messages at scale.
	• Developing AI agents and an agentic workflow to automate the above processes, enabling the automation of form filling, audio calls and the generation of documents to enable abuse at scale. The use of agentic AI reduces the amount of effort from the attacker's perspective due to being objective based as opposed to requiring specific prompts to generate output.
	It has also been found that the OCG has access to tools that can:

<table>
<tr><td></td><td colspan="6">

Fabricate mock transactions (e.g. payslip deposits, rent payments) to simulate legitimate use and evade early anti-money laundering flags.
Plan transaction patterns mimicking genuine customer behaviour (e.g. round-number avoidance, consistent time-of-day activity).
Create online personas with fake LinkedIn, Facebook, and email histories that appear consistent with identity documents.
Automate the operation of the above using a combination of traditional automation and agentic AI to enable greater complexity and scale of operations.

</td></tr>
<tr><td>Impact (Incl. Scale)</td><td colspan="6">

Following an investigation into an unauthorised account creation, the firm has identified a vulnerability in a widely used identity verification tool, which has enabled an attacker to create multiple fraudulent customer accounts, believed to be linked to potential money laundering and fraud activities. It is assessed that the vulnerability has existed for some time and enabled the attacker to create multiple fraudulent customer accounts.
The firm is now unsure of the legitimacy of customer accounts created during that period and the activities linked to them.
As a result, there is potential for extensive consumer harm, safety and soundness or financial stability impacts through disruption to new account creation, material loan defaults, illegitimate market movements, or reputational/confidence issues.
Other firms are then informed of the vulnerability with some increase the controls on any transition to for from the impacted firm and, in some case, to suspend activity altogether.
Following broader investigations, it transpires that the tool is widely used across the sector.
Implementing real-time validation and increasing human interaction in the identification and verification process has resulted in longer validation times. This has led to temporary delays in account creation and onboarding, causing frustration among new customers and potential clients.
It is later discovered that the attacker has a reinforcement learning loop, which allows them to submit failed applications back into the system to improve future attempts via LLM-driven revision.
Leaks about the potential freezing of new customer accounts and the effectiveness of internal mitigation control have spread on social media, causing widespread concern, reputational damage, and the possibility of a surge in withdrawals.

</td></tr>
<tr><td>[Risk] Coverage</td><td>People
☐</td><td>Property
☐</td><td>Technology
☒</td><td>Data (Availability)
☒</td><td>Data (Integrity)
☒</td><td>Third Party
☒</td></tr>
<tr><td>Characteristics</td><td colspan="6">

Rapid onset - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place.
Low predictability/highly changeable - Threat Actor adapts to counter moves.
High persistence - potential for recurring periods of disruption.
Information asymmetry - key information regarding the incident may not be fully visible.

</td></tr>
</table>

Assumptions	• Incident happens on a peak and/or significant trading day with above average volume (in line with the worst-case scenario used for setting impact tolerance). • The OCG is a capable attacker with motive and means to act at scale. • Account reset options are likely to be highly complex and/or require significant manual intervention.			
Stress Variables				
Account impact	Staff ☐	Third Party ☐	- ☐	- ☐
Vulnerability age	3 Days ☐	1 Week ☐	2 Weeks ☐	1 – 3 Month ☐
Account Volumes	<10 ☐	<100 ☐	<1000 ☐	>1000 ☐
Identity Validation	Synchronous ☐	Asynchronous ☐	- ☐	- ☐
Other	Attacks could include using Gen-AI for: • Creation of fake ID for a fictitious person • Creation of fake ID for a real individual • Social engineering attack on a legitimate user and account An additional stress variable could consider material loan defaults or illegitimate market movements resulting from this attack, leading to wider market disruption and confidence impacts to the UK sector more broadly.			

Technology & Data (Non-Cyber)

Poorly Executed Change	**Scenario Category**
	Technology & Data (Non-Cyber)

Scenario Description	
Overview	This Scenario explores a significant data corruption event following a poorly executed [routine or emergency] change that impacts a critical piece of core [storage] infrastructure supporting multiple IBS.
Cause	Following an overnight emergency change, system abnormalities are identified in the post change technical check out and a decision is made by Technology to attempt to roll back to the original version ahead of start of business. However, a mistake in the roll-back process results in a significant amount of data corruption impacting a number of downstream applications.
Impact (Incl. Scale)	• A high volume of users report abnormal and inconsistent data, including [customer account and/or transaction/ payment] related data, across internal and customer facing applications. • Customers report the issue through other channels and the volume of enquires begin to overwhelm all customer channels. • As there is little confidence left in the integrity of the data the only remaining option is to shut down the impacted systems and undertake a full-scale system recovery. • Attempted recovery from the incident is complicated as the corruption appears to have been propagated via the normal data replication process to the redundant pair meaning recovery will be required from [tape] back-ups, and the reconstitution of a proportion of critical data [from backups/logs/reconstitution from other sources]. • Further delays are then experienced due to the high volume of data recovery attempted via the backup and restore process. • During Incident calls, technology recovery teams have highlighted the potential nonalignment of data based on the likely data recovery point necessitating technical and business reconciliation activity post data restoration from back-ups. • As a result, key systems are likely to be offline for a minimum of **[2]** business days. **(SV)** • Incident is not believed to be cyber related, and no abnormal behaviour has been reported by the Security Operations Centre who have deployed heightened monitoring.

[Risk] Coverage	People ☐	Property ☐	Technology ☒	Data (Availability) ☒	Data (Integrity) ☒	Third Party ☐

Characteristics	
	• **Rapid onset** - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place. • **Uncertain duration** of investigation, containment and recovery time makes estimating business recovery times difficult. • **Higher scrutiny** and potential to undermine stakeholder trust - through perceived or actual lack of action/transparency due to nature of incident.

	• **Other:** Infrastructure failures often manifest in previously unknown ways and other concurrent but separate IT issues may be conflated, distracting recovery teams.				
Assumptions	• Incident happens ahead of a peak and/ or significant trading day with above average volume. • The scenario assumes that technology change controls have failed. • There is no cyber activity associated with this scenario.				
Stress variables *(illustrative levels, to be adjusted as appropriate)*					
Duration of outage	3 days ☐	4 days ☐	1 week ☐	2 weeks ☐	>2 weeks ☐
Type of data impacted	Personal ☐		Financial ☐		Sensitive ☐
Other	Customer data is merged, resulting in data being displayed to the wrong customers resulting in data confidentiality breaches				
Case Study					
Causation/ Impact (Risk Coverage):	On 19th Jul 24, CrowdStrike, a third-party cybersecurity company, distributed a faulty update following a poorly executed change to its Falcon Sensor security (vulnerability scanning) software, resulting in widespread unavailability of technology (principally those running MS Operating Systems)				
Impact (scale):	Approximately 8.5 million systems were impacted across multiple sectors, including financial services, disrupting both the private sector and public sector organisation and services including transportation.				
Duration:	Although the error was discovered and a fix released within hours, many computers required manual interventions prolonging the outage for some services over several days.				
Compound Scenario Considerations:	For some organisations in the US, the impact from the CrowdStrike change exacerbated the impact from the previous day's disruption to MS Azure Cloud Services (which impacted MS365 and other services).				
Takeaways:	The incident highlighted the potential for disruption caused by third party software updates to impact a firm and other third parties they rely on, meaning firms need to consider simultaneous internal disruption and disruption to one or more third parties. It also highlighted potential shortfalls with robustness of a firms own controls to manage sources of disruption from third Party software providers and in certain circumstances, the challenge of high-volume manual interventions which raises questions over firms' ability to mobilise the required (skilled) resources to execute a timely recovery.				

Physical Security

<table>
<tr><td colspan="5">Terrorism - Marauding Armed Intruders</td><td>Scenario Category</td></tr>
<tr><td colspan="5"></td><td>Physical Security</td></tr>
<tr><td colspan="6">Scenario Description</td></tr>
<tr><td>Overview</td><td colspan="5">This Scenario explores the impact of Terrorism - Marauding Armed Intruders, resulting in the disruption of essential properties and people related services with a focus on associated safety challenges.</td></tr>
<tr><td>Cause</td><td colspan="5">Single/multiple armed intruders launch an attack in a density populated area within close proximity of financial services buildings.</td></tr>
<tr><td>Impact
(Incl. Scale)</td><td colspan="5">• In the short period before emergency services are able to deploy, contain, then neutralise the threat, armed intruders exploit the element of surprise and panic to move freely around the area.
• Despite the invocation of lock down and other emergency protocols, armed intruders manage to enter buildings with resultant damage to property and risk to life.
• Firms struggle to establish situational awareness and account for staff, hampered by public communication channels taken offline to avoid network congestion for emergency responders, lasting up to 24 hours.
• Despite this, images and videos quickly emerge and are circulated widely on social media and news outlets.
• Following the attack, police cordons remain, with all commercial buildings situated within specific radius of attack site closed for up to [14] days to facilitate criminal investigations and damage assessment.
• Transport networks are significantly impacted to and from the site and broader area, with road closures and public transport severely disrupted due to police presence. For some routes, restrictions remain for [x]days.
• Elevated levels of public and staff anxiety persist, with higher police presence remaining in place for days after the attack due to policy intelligence indicating further attacks.
• Impacted firms complete accounting for staff procedures. [20] % staff, including those identified as critical to the operating of IBS, are expected to be unable to return to work resulting from either being directly or indirectly impacted by the events.
• Increased media exposure of targeted organisation leading to scrutiny and unfounded claims being made online.</td></tr>
<tr><td>[Risk] Coverage</td><td>People
☒</td><td>Property
☒</td><td>Technology
☐</td><td>Data (Availability)
☐</td><td>Data (Integrity)
☐</td><td>Third Party
☒</td></tr>
<tr><td>Characteristics</td><td colspan="5">• Rapid onset - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place.
• Low predictability/highly changeable - the Threat Actor(s) adapts to counter moves.
• Information asymmetry - key information regarding the incident may not be fully visible.
• Disrupted Communication - Internal and external communication channels are impaired by the nature of the incident.
• Elevated Staff anxiety resulting from actual or perceived threat to safety of staff and/or family members and concerns over firm stability.</td></tr>
</table>

	• **High persistence** - potential for recurring periods of disruption (e.g. secondary attacks). • **Other**: Typically focused on high population centres, landmarks, or areas of heightened government / public interest.				
Assumptions	• Incident happens ahead of peak and/ or significant trading day with above average volume. • Event has had a profound impact on the mental health of the workforce.				
Stress variables *(illustrative levels, to be adjusted as appropriate)*					
Secondary Attacks	Yes ☐	No ☐	- ☐	- ☐	- ☐
# of Impacted Sites	Single ☐	Multiple ☐	Campus ☐	Country Wide ☐	- ☐
Building Unavailability	1-2 days ☐	3-5 days ☐	5-14 days ☐	14-30 days ☐	30 days+ ☐
Staff Absence (at impacted sites)	20% ☐	30% ☐	40% ☐	50% ☐	50%+ ☐
Case Study					
Causation/ Impact (Risk Coverage):	Geopolitical tensions between India and Pakistan over the Kashmir region contributing to the rise of groups like Lashkar-e-Taiba "Let". In November of 2008, Mumbai suffered a brutal series of 12 coordinated attacks across the city, when 10 members of LeT carried out shootings and bombing attacks.				
Impact (scale):	A total of 175 people died, including nine attackers, with more than 300 injured across the city. The scale and brutality of the assault shocked the world and highlighted vulnerabilities in the India's security and emergency response. Hotels, transport links and one hospital (Cama Hospital) were all targeted.				
Duration:	The attacks lasted for 3 days between 26th - 29th of Nov. 2008. However, the impacts persisted beyond due to the fear of a secondary wave of attacks.				
Compound Scenario Considerations:	Multi locations: Not just one city like Mumbai. And Multi mode attacks: High-profile locations, armed assaults, hostage situations, and bombings. Soft Target vulnerability: Hotels, hospitals, transport are typically lightly defended yet densely populated. Disruption on Information overload: Attacks come with a surge of information, unstructured and overwhelming, this can cause unclear and wrong decision making leading to more damage. Hostage situations: The prolonged nature of hostage situations can cause days/weeks of damage to public wellbeing and create sociological damage				

Takeaways:	Internationally, the attacks underscored the global threat of terrorism, prompting a call for stronger international cooperation on security, intelligence sharing and anti-terrorism strategies. India creating the National Investigation Agency (NIA) for specialized investigation of terrorism related cases. Strengthening Intelligence and Communication. The attacks exposed gaps in intelligence sharing, leading to improved coordination among intelligence and security agencies. Improved Crisis Responses: Training and equipping local police and rapid response forces become a priority.

Terrorism - Mass Destruction	Scenario Category
	Physical Security

Scenario Description	
Overview	This Scenario explores a terrorism mass destruction attack directed at Financial Services, resulting in the total loss of the impacted building(s) and the unavailability of core teams/individuals supporting IBS.
Cause	Terrorists detonate a (single/multiple] large improvised explosive device(s) directly outside/in close proximity to [insert firm] location, resulting in damage to the building and resultant risk to life.
Impact (Incl. Scale)	• The explosion causes extensive damage to both the buildings in the immediate vicinity of the blast but also to surrounding buildings within a [500]-meter radius. • Emergency Services are deployed, and inner and outer cordons raised and routes in and out of the area are closed to facilitate evacuations. • Emergency evacuations, where undertaken, are extremely challenging, both due to the nature of the attack and the multiple buildings impacted, resulting in large numbers of people attempting to move to Emergency Evacuation (EV) points / dispersing within the wider area. • Where appropriate, buildings in the wider areas invoke invocation procedures to protect staff from any secondary attack / falling debris from damaged buildings. • Firms struggle to establish situational awareness and account for staff, hampered by public communication channels taken offline to avoid network congestion for emergency responders, lasting up to 24 hours. • Some of the most impacted buildings suffer partial collapse due to the extent of structural damage and are likely to be unavailable for a prolonged period [x months] / indefinitely. Even where damage appears less extensive, full assessment make take weeks to undertaken following. • In addition to the immediate vicinity, transport networks are significantly impacted to the broader area, with road closures and public transport being severely disrupted due to police presence. For some routes, restrictions remain for [x]days. • Elevated levels of public and staff anxiety persist with higher police presence remaining. Several terrorist organisations claim responsibility and threaten attacks in other locations. The [UK] Threat Level adjusts to reflect this, and firms implement heighten security measures in other locations. See stress variables. • Due to the nature of the attack, staff may be directly or indirectly impacted and [30] % staff, including those identified as critical to the operating of IBS, are expected to be unable to return to work resulting from either being directly or indirectly impacted by the events. For smaller, collocated teams, the entire team may be unavailable for at least [48-72] hrs. Departments report a material drop in productivity more broadly of up to [30%] due to distress.

[Risk] Coverage	People ☒	Property ☒	Technology ☐	Data (Availability) ☐	Data (Integrity) ☐	Third Party ☐

Characteristics	• **Rapid onset** - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place. • **Low predictability/highly changeable** - the Threat Actor(s) adapts to counter moves.

	• **Information asymmetry** - key information regarding the incident may not be fully visible. • **Disrupted Communication** - Internal and external communication channels are impaired by the nature of the incident. • **Elevated Staff anxiety** resulting from actual or perceived threat to safety of staff and/or family members and concerns over firm stability. • **High persistence** - potential for recurring periods of disruption (e.g. secondary attacks). • **Other**: Typically focused on high population centres, landmarks, or areas of heightened government / public interest.				
Assumptions	• Incident happens on a peak and/or significant trading day with above average volume (in line with the worst-case scenario used for setting impact tolerance). • Event has had a profound impact on the mental health of the workforce.				
Stress variables *(illustrative levels, to be adjusted as appropriate)*					
Secondary Attacks	Yes ☐	No ☐	- ☐	- ☐	- ☐
# of Impacted Sites	Single ☐	Multiple ☒	Campus ☐	Country Wide ☐	- ☐
Building Unavailability	3 months ☐	6 months ☐	9 months ☐	12 months ☐	18 months ☐
Staff Absence (at impacted sites)	30% ☐	40% ☐	50% ☐	50%+ ☐	Whole Team ☐
Productivity impact	<25% ☐	25 - 50% ☐	50% ☐	50% - 75% ☐	75%-100% ☐
Case Study					
Causation/ Impact (Risk Coverage):	11 September 2001 Al-Qaeda hijacked four commercial airplanes, deliberately crashing two of the plans into the North & South Towers of the World Trade Centres, resulting in the collapse of both towers and WTC7 with extensive damage to properties adjacent. The attack resulted in the largest loss of life from a terrorist incident along with considerable long-term impacts to people both directly and indirectly effected.				
Impact (scale):	The scale of the impact was unprecedented, and it remains the largest terrorist attack in terms of lives lost, extent of the physical damage and the duration in terms of the denial of access to business premises. The NYSE closed for 7 days.				
Duration:	Although the attacks took place on 9/11, the duration of the incident was measured in weeks/months depending on the specific location and level of damage firms sustained This does not include the longer-term impacts to staff.				
Compound Scenario Considerations:	For firms planning for a long-term unavailability of premises or critical team, work transference to other sites with the appropriate capacity, skills and technology will be an important response and recovery strategy, as will WFH for those staff still able to work. Therefore, any technology incident that impacts				

	remote working or which impacts the receiving site/team can be considered as a way of compounding such a scenario
Takeaways:	Large scale mass destruction attacks represent some of the most impactful incidents in terms of consequences on a firm's staff, customers, and society at large. They are, by their nature, extremely destructive to the physical assets impacted (e.g. buildings) albeit in a relatively small geographic area. Beyond the priority of staff / customer safety and wellbeing, firms need to consider the impact to IBS, particularly where critical aspects of the IBS are concentrated in higher risk location e.g. single location teams, co-location of people and technology and proximity or limited transit options to recovery sites. Recovery may be measured in weeks/months and therefore the sustainability of response and recovery strategies needs to reflect the risk they are designed to mitigate.

Civil Unrest	Scenario Category
	Physical Security

Scenario Description	
Overview	This Scenario explores the impact of civil unrest, which, in addition to the disruption of essential public services, results in the unavailability of personnel and premises critical to the functioning of IBS.
Cause	Following a period of rising social tension due to [aggravating factors relevant to geographical region/political and social context], a [trigger event] causes widespread civil unrest in [country/region] threaten to overwhelm essential services.
Impact (Incl. Scale)	• Large protests gather outside of significant buildings, such as government and sensitive/cultural locations, as well as areas in which protestors feel they will gain significant media coverage. • This includes major financial hubs where banks become primary targets of public anger resulting in closures to protect customers and employees. • There are widespread instances of protest turning violent. • Transport networks are significantly impacted in urban centres, with roads becoming unpassable and public transport being severely disrupted due to protests and criminal damage. This will last for [5] days. • Local businesses suffer extensive property damage, looting and closures due to the unrest, with many unable to afford the repair and reopening costs. • There is a high risk to public safety due to the stretched police and medical services and the violence occurring in the streets. • Health & Safety of workforce is a legitimate concern, whether they are on-site or at home. • High levels of employee absenteeism of up to [xx%] are reported in urban locations where the unrest has focused. • As emergency service struggle to regain control, there is a risk of civil unrest spreading beyond just the major urban centres.

[Risk] Coverage	People	Property	Technology	Data (Availability)	Data (Integrity)	Third Party
	☒	☒	☐	☐	☐	☒

Characteristics	• **Slower onset** - Longer lead time provide potential for pre onset actions. Note: depending on the cause and nature, civil unrest can be spontaneous however it is often proceeded by identifiable causal factors/events allowing for a period of preparation. • **Low predictability / highly changeable** – crowds / any threat actors adapt to the changing situation. Local instances / offshoots can occur with little or no notice and spread rapidly. • **Elevated Staff anxiety** - resulting from actual or perceived threat to safety of staff and/or family members and concerns over firm stability. • **Conflicting priorities** - During incidents with potential broader societal impacts, staff may face competing prioritise regarding family/caring responsibility, limiting their ability to work/support the firms response. • **Other:** Typically focused on highly population density areas and notable landmarks (associated with the focus on discontent).
Assumptions	• Incident happens ahead of peak and/ or significant trading day with above average volume.

	• Branches have been damaged and will be forced to close for up to 1 month. • Event has left many customers financially vulnerable due to damage/destruction of possessions. • Some external suppliers are heavily impacted as well.				
Stress variables *(illustrative levels, to be adjusted as appropriate)*					
# of Impacted Sites	Single ☐	Multiple ☐	Campus ☐	Country Wide ☐	- ☐
Building Unavailability	1-2 days ☐	3-5 days ☐	5-14 days ☐	14-30 days ☐	30 days+ ☐
Staff Absence (at impacted sites)	20% ☐	30% ☐	40% ☐	50% ☐	50%+ ☐
Case Study					
Causation/ Impact (Risk Coverage):	On the 25th of May 2020, in Minneapolis, Minnesota man named George Floyd was killed by a police officer that knelt on his neck for over nine minutes after being arrested. Footage of the event was captured and shared online, sparking large scale protests and civil unrest				
Impact (scale):	Large, sustained protests unified under the Black Lives Matter (BLM) movement began in Minneapolis and quickly spread across the U.S. and internationally, becoming some of the largest protests in recent history. Some of the protests escalated into confrontations, leading to property damage, looting, and curfews in cities throughout the U.S. The unrest led to the death of 19 people, and the damage amounted to $1-2 billion.				
Duration:	The most intense period of civil unrest lasted about two weeks, between the end of May and beginning of June. Public demonstrations and activism continued for months after the event.				
Compound Scenario Considerations:	Several compounding factors intensified the civil unrest following George Floyd's death. Firstly, this was not an isolated incident but part of a series of high-profile cases of police violence against Black Americans. The COVID-19 pandemic added to public frustration with government institutions, while increased political polarization in the lead-up to the 2020 presidential election heightened tensions. Together these factors created the social, economic, and political conditions that fuelled the intense civil unrest seen during the George Floyd protests.				
Takeaways:	The George Floyd protests highlighted how rapidly longstanding issues can compound and escalate into widespread unrest, emphasizing the need for rapid response capabilities. This widespread unrest can be significantly amplified due to the prevenance of social media. Effective monitoring of social media can be used as a risk indicator and a tool for understanding public sentiment and gauging potential unrest. Especially when dealing with the public, transparency and accountability should be prioritised. A need to improve understanding of how separate issues can intersect and compound to worsen the impact of a disruption. The protests demonstrated the importance of safeguarding both employees and assets. Business continuity plans should address physical security, remote working options, and clear communication protocols.				

Geopolitical

Disruption to Undersea Cables	**Scenario Category**
	Geopolitical

Scenario Description						
Overview	This scenario considers a significant coordinated attack aimed at disrupting the internet connectivity of a state/region. NB: Although this would be highly unlikely and unprecedented, an attack of this scale provides an opportunity to explore response options and alternate solutions. More likely scenarios are faults or accidental impacts to undersea cables and 100 occur each year but with little or no impact. Similarly, a sabotage impacting one to three cables would have a lower impact due to alternate routes with sufficient bandwidth to manage peak loads.					
Cause	Following increase geopolitical tensions, a hostile state actor in coordination with proxy(ies) actors damage several undersea cables at a known checkpoint and/or their endpoints to disrupt internet communications for targeted countries. Ongoing security challenges result in significant time to access and repair the damage, prolonging the disruption. Scenario cyber variation: The physical damage to cables is followed by a coordinated cyber-attack by the state actor/proxies designed to further disrupt data flows by targeting the systems and software designed to manage the automatic re-routing of data. Alternate (Geohazard): outside of a highly coordinated sabotage scenario, an earthquake represents a plausible scenario that results in multiple cable breaks and potential compound scenario were combined with a series of sabotage events.					
Impact (Incl. Scale)	• Firms across all sectors within the impacted [country / region] experience temporary loss of internet service as automated and manual re-routing attempts to allow the flow of data across alternative routes. Despite these measures (which utilise in built resilience /redundancy), firms experience degraded service across internet connectivity and/or telephone traffic with an average loss of **[25%]** of band width reported across **[2-3 days]** requiring traffic reprioritisation**. (SV)** • Firms also report the loss of access to data and applications hosted in other countries / regions for the same time period. **(SV)** • As impacts are broad based across all sectors, critical third parties supporting IBS report a drop in services levels **(SV)**					
[Risk] Coverage	People ☐	Property ☐	Technology ☒	Data (Availability) ☒	Data (Integrity) ☐	Third Party ☒
Characteristics	• **Rapid Onset** - this is a no-notice event little to no time to put additional mitigations in place.					

	• **Low predictability / highly changeable** - Threat actor(s) adapts to counter moves. • **High persistence** - potential for recurring periods of disruption • **Information asymmetry** - key information regarding the incident may not be fully visible. • **Disrupted Communication** - Internal and external communication channels are impaired by the nature of the incident.				
Assumptions	• Incident happens ahead of a peak and/ or significant trading day with above average volume. • Highly capable nation state actor who accepts the potential consequences of this action. • Impacts are felt across all sectors.				
Stress variables *(illustrative levels, to be adjusted as appropriate)*					
Bandwidth Degradation	30% ☐	40% ☐	50% ☐	60% ☐	>60% ☐
Duration	2-3 days ☐	<1 week ☐	2 weeks ☐	3 weeks ☐	1 month ☐
Access offshore hosted locations	80% ☐	60% ☐	40% ☐	20% ☐	None ☐
Case Study 1					
Causation/ Impact (Risk Coverage):	In FEB24, three undersea cables were damaged in the Red Sea. Whilst not conclusively ascertained to be deliberate intervention, Yemini government warned in early FEB23 that Houthi rebels may attack undersea cable infrastructure. US Intelligence later suggested that the cables were damaged by the anchor of a sinking ship which had been struck by a Houthi missile on 18th Feb 24.[4]				
Impact (scale):	It is estimated that 25% of traffic between Asia, Europe, and the Middle East were impacted as a result. In BAU, cables in the Red Sea are estimated to support ~80% of total west bound communications between Europe and Asia.[5]				
Duration:	Whilst rerouting meant that the impact of the incident was contained, the repairs on the undersea cables were not fully complete until Jul 2024, 5 months after the initial incident.				

[4] CBS News. Ship sunk by Houthis likely responsible for damaging 3 telecommunications cables under the Red Sea. Available [Online]: Ship sunk by Houthis likely responsible for damaging 3 telecommunications cables under Red Sea - CBS News (06/03/24).
[5] BBC. Crucial Red Sea data cables cut, telecoms firm says. Available [Online]: Crucial Red Sea data cables cut, telecoms firm says - BBC News (05/03/24)

Compound Scenario Considerations:	Cyberattacks can often accompany other forms of action either in direct support or as other threat actors seek to exploit other incidents to their advantage. Therefore, it is highly plausible for cyberattacks on Critical (Inter) National Infrastructure during a broader geopolitical event.
Takeaways:	Due to the complex nature of undersea cable damage investigations, undersea cable disruptions are unlikely to conclusively be attributed to nation state actors or associated groups. However, whilst a coordinated, geographically dispersed attack on cable infrastructure is highly unlikely it is plausible.
Case Study 2	
Causation/ Impact (Risk Coverage):	On the 26th Dec 06, the 7.1 magnitude Hengchun earthquake and subsequent aftershocks south of Taiwan caused 22 recorded failures across 9 undersea cables in the region. [6]
Impact (scale):	As a result, there was widespread impact to telecommunication / internet-based traffic across Taiwan, Singapore, Hong Kong, South Korea and Japan including reports of some disruption to financial services including trading-based activity in Hong Kong where traders were unable to obtain prices and complete orders due to network issues.
Duration:	Following the initial earthquake, it took 49 days to fully recover from all the damaged cables. The remediation timeline was elongated due to the number of faults, availability of cable repair vessels, adverse sea conditions, and the depth of the cables (up to 4000m deep) – some of which were buried under mud due to underwater landslides.[7]
Compound Scenario Considerations:	Large scale geohazard are frequently multifaceted in the impact caused. As such, there are a range of possibilities for combining impact causation types. In the case of an Earthquake like Hengchun, impacts to technology and data are like to accompany other impacts to people and premise and society more broadly.
Takeaways:	Although redundancy and re-routing generally affords a level of resilience to the disruption to underseas cables this case study demonstrates the plausibility in the loss of multiple cables simultaneously and the impact either in terms of a complete disruption to some network traffic or latency issues resulting from traffic trying to re-route through a lower number of cables.

[6] International Cable Protection Committee (ICPC). Press Release - Subsea Landslide is Likely Cause of SE Asian Communications Failure. Available [Online]: file:///C:/Users/45181694/AppData/Local/Temp/MicrosoftEdgeDownloads/70ea5d64-dfcb-49cc-b925-039fe06dcaf5/ICPC_Press_Release_Hengchun_Earthquake.pdf (21/03/2007)

[7] *ibid*

Natural Hazards & Public Health

Severe Weather	**Scenario Category**
	Natural Hazards & Public Health

Scenario Description						
Overview	This Scenario explores the impact of severe weather, resulting in widespread disruptions to infrastructure, transportation, and utilities.					
Cause	A combination of extreme meteorological conditions, including storms, heavy rainfall and strong winds. This is driven by natural climate variability but is intensified by global climate change.					
Impact (Incl. Scale)	• Despite being closely tracking by meteorological agencies over several days, a [severe storm/superstorm/typhoon etc] departs from its expected trajectory and rapidly gains intensity [insert category] as it makes landfall. • Transport networks are significantly impacted throughout large parts of the [region/country]. Roads, bridges, and railways are blocked due to flooding, fallen debris and damage to infrastructure. Even where routes are clear, transport operators struggle with staff shorts forcing services to be suspended. Key routes are expected to be closed for 2-3 days with some more localised routes impassable for up to 7 days. The public has been advised not to travel unless it is critical. • The situation is further exacerbated as emergency services and repair teams are hampered by a lack of communications and an inability to fully access impacted areas. • Regional energy blackouts are occurring with a restoration of services expected to take up to [5] days in places. *See Stress Variables and NPO scenario.* • Telecommunication infrastructure has been hit particularly hard with damage to cell towers that have been brought down due to the extreme wind speeds – full recovery of services is estimated to take over a week. • Even for businesses able to maintain power to their buildings through Unlimited Power Supplies (UPS)/generators, access to the internet and other communications channels is down or severely limited. • Health & Safety of workforce is a legitimate concern, whether they are on-site or at home. The severe weather and its after-effects pose a significant risk to life. • Widespread school/childcare closures for up to 7 days • The aggregate impact of disruption to transportation, telecommunications including the internet and caring responsibilities, results in elevated staff absence of up to 20%. *See Stress Variables* • Due to safe consideration and disruption to market participants the market/trading has been suspended. *See Stress Variables*					
[Risk] Coverage	People ☒	Property ☒	Technology ☒	Data (Availability) ☐	Data (Integrity) ☐	Third Party ☒
Characteristics	• **Slow(er) onset** - Longer lead time provide potential for pre onset actions. • **Elevated Staff anxiety** - resulting from actual or perceived threat to safety of staff and/or family members and concerns over firm stability.					

	• **Conflicting priorities** - During incidents with potential broader societal impacts, staff may face competing prioritise regarding family/caring responsibility, limiting their ability to work/support the firms response. • **Disrupted Communication** - Internal and external communication channels are impaired by the nature of the incident. • **Other:** Elevated risk from compound scenarios through greater reliance on technology and the likely impact from the weather event
Assumptions	• Incident happens ahead of peak and/ or significant trading day with above average volume. • UPS/Generators will work as expected to facilitate shutdowns and evacuations. • A number of branches have been damaged and will be forced to close for up to 1 month. • Event has left many customers financially vulnerable due to damage/destruction of possessions. • External suppliers are heavily impacted as well

Stress variables *(illustrative levels, to be adjusted as appropriate)*					
Market Status	Mkt. Open ☒	Mkt. Closed (1 day) ☐	Mkt. Closed (2 days) ☐	Mkt. Closed (3 days) ☐	Mkt. Closed (4+ days) ☐
Utilities Impact (Power)	Local (1-2 days) ☐	Regional (1-2 days) ☐	Local (3-5 days) ☐	Regional (3-5 days) ☐	5 days + ☐
Utilities Impact (Telecoms)	Mobile ☐	Network ☐	-	-	-
Staff absence	20% ☐	30% ☐	40% ☐	50% ☐	-
Physical Security	Localised unrest ☐	Widespread unrest ☐	Targeting of FS Firms ☐	-	-

Case Study	
Causation/ Impact (Risk Coverage):	Hurricane Katrina hit the U.S. Gulf Coast on the August 29, 2005, as a Category 3 storm, bringing extreme winds, heavy rainfall, and a storm surge that overwhelmed levees in New Orleans. Despite the evacuation efforts, thousands of residents remained because they lacked the means to leave, while approximately 80% of the city became inundated with floodwaters.
Impact (scale):	Much of New Orleans was destroyed, over 1,800 people died and tens of thousands were left homeless and without basic supplies. Persistent flooding led to widespread lethal pollution and the destruction of 90% of the essential utility networks (energy, communications, water etc.). Over 1 million people were displaced from the Gulf Coast region, and many communities in New Orleans faced permanent population decline. The economic loss estimates from Hurricane Katrina are $125 Billion.

Duration:	The immediate weather-related impacts lasted approximately 1 week, exacerbated by a slow and fragmented response. The recovery and rebuilding efforts continued for years. Full recovery of infrastructure, housing, and public services took over a decade in some areas.
Compound Scenario Considerations:	Hurricane Katrina's impacts were compounded by failures in infrastructure, economic and health consequences, social vulnerabilities, and insufficient public services. As a result, the severity of the weather event was amplified significantly.
Takeaways:	Hurricane Katrina highlighted the importance of infrastructure resilience, particularly for flood protection systems, and the need for regular maintenance and upgrades to meet the level of risk. It puts a specific focus on ensuring that preparedness and plans are suitable for all, especially those classed as vulnerable. And that this preparedness should consider the impact of compounding factors. Response should be underpinned by clear coordination and communication. Given the increasing extreme weather events, Katrina emphasizes the need to integrate climate change adaptation into disaster planning to better withstand future risks.

Global Pandemic	Scenario Category
	Natural Hazards & Public Health

Scenario Description	
Overview	This Scenario explores the impact of a global infectious disease pandemic, resulting in widespread governmental interventions to contain the spread including local and/or countrywide lockdowns, travel restrictions and healthcare rationing.
Cause	The source of the pandemic remains unknown but appears to have originated from [insert origin], spreading more rapidly than previous pandemics, resulting in cases confirmed across all regions within a matter of [x] weeks.
Impact (Incl. Scale)	• The progression of the pandemic is non liner with 2-3 waves (of between 12-15 weeks) with different levels of severity. • Despite government and firm measures in response, staff absentee rates reach significantly elevated levels for a sustained time, exacerbated as the disease spreads during a winter where populations are already experiencing above normal levels of flu illness and mortality. • Team leaders report absence driven by direct illness, caring responsibilities, and mental health impacts. At its height, several locations experience a peak of 30-35% absence across a two-to-three-week period within larger teams, with some smaller teams reaching 50% absence for the same period. **(SV)** • All teams experience a base minimum of 20%. **(SV)** • The move to predominantly remote working puts a great reliance on local power/telecoms infrastructure and firms' remote access networks with cyber risks elevated. **(SV)** • There is an increased risk to vulnerable customers as certain channels are closed or restricted e.g. Branch and Call Centers and their wider support networks are also constrained by the impacts to broader society. • These impacts are felt equally on the firm's third parties and other market participants compounding operational challenges. **(SV)** • [Insert Third Party] reports that local government restrictions, combined with absentee rates are resulting in a [insert value] drop-in service. **(SV)**

[Risk] Coverage	People	Property	Technology	Data (Availability)	Data (Integrity)	Third Party
	☒	☒	☒	☐	☐	☒

Characteristics	• **Slow(er) onset** - Longer lead time provide potential for pre onset actions. • **Chronic by nature** placing a greater emphasis on sustainability of recovery strategies. • **Elevated Staff anxiety** - resulting from actual or perceived threat to safety of staff and/or family members and concerns over firm stability. • **Conflicting priorities** - During incidents with potential broader societal impacts, staff may face competing prioritise regarding family/caring responsibility, limiting their ability to work/support the firms response. • **Pan regional** impacts may limit use of transference strategies. • **Other:** Elevated risk from compound scenarios through greater reliance on technology
Assumptions	• Incident happens ahead of peak and/ or significant trading day with above average volume.

	• All locations that an IBS operates from are in some level of lockdown, meaning only staff supporting activity deemed essential to the economy are permitted to work from the office, although almost all remote working enabled staff are WFH. • Although rates of absence are unlikely to be uniform across a regions or county with peak absence at different times, an even absence level should be assumed to reflect the inability to predict how the distribution of high levels of absence will play out. Scenario should additionally consider the availability of 'critical personnel' required during the discovery/recovery/remediation of the incident, such as SMEs, decisionmakers, and material risk takers. • Number of vulnerable customers is elevated as lockdown increases instances of financial and personal vulnerabilities.

Stress variables *(illustrative levels, to be adjusted as appropriate)*					
Staff Absence (All teams)	20% ☐	35% ☐	50% ☐	N/A ☐	N/A ☐
Staff Absence (Most impacted)	35% ☐	50% ☐	50 - 60% ☐	60-70% ☐	>70% ☐
Duration of lockdowns /	2-4 weeks ☐	4-8 weeks ☐	8-12 weeks ☐	6 months ☐	1 year ☐
Movement Restrictions	No x-border ☐		No intra state ☐		Full ☐
Third Party Service Impact	<25% ☐	25 - 50% ☐	50% ☐	50% - 75% ☐	Stressed exit ☐
Third Party Coverage	None ☐	One ☐	Some ☐	Most ☐	All ☐

Case Study	
Causation/ Impact (Risk Coverage):	COVID-19 first appeared on a small scale in NOV19 with the first large cluster appearing in Wuhan, China, in Dec 2019. The subsequent worldwide transmission caused a pandemic to be declared 11MAR20, by the World Health Organization (WHO). In response, the UK government closed schools on 20th Mar 20 and lockdown regulations came into effect 26th Mar 20.
Impact (scale):	In the UK 25% of companies had to temporarily close during covid and homeworking doubled to 9.9m with many organisations having to rapidly increase their working from home capability. It is estimated that Covid-19 lowered total factor productivity in the UK private sector by up to 5%. While critical sectors such as financial services continued operating on-site where essential during lockdown, working remotely was rapidly implemented across all other services wherever feasible. Firms had to quickly adapt not only their working practices but also the systems and controls needed to ensure that services delivered remotely continued to meet the regulatory and risk management standards. These changes had to be implemented while firms also worked to support evolving and heightened customer needs, including those of vulnerable individuals impacted by the pandemic.
Duration:	The pandemic remained a global health emergency from Mar 20 to May 23. Within the UK there were two lockdowns from Mar 20 to Jun 20 and Dec 20 to

	Mar 21. Restrictions remained in place, including social distancing and isolation until Apr 22 when all restrictions were stopped.
Compound Scenario Considerations:	COVID-19 changed the resource/asset mix that underpin services and the way customers accessed them, with many of these changes have remaining. As such, any pandemic scenarios that considered a return to, and the resilience of, homeworking can be compounded with technology issues that disrupt the contingencies invoked e.g. network disruption. Furthermore, although staff absence was elevated, this did not reach the high levels of some of the contingency plans. As scenario such as pandemic where society wide, the failure of a Third Party provides another avenue to explore compound impacts to a firms Important Business Services.
Takeaways:	The crisis accelerated unprecedented transformation as organisations responded to the pandemic. It altered work traditions and paradigms challenging long held assumptions on severity and plausibility of scenarios that should be planned for and the parameters upon which contingencies are based e.g. the pandemic showed that both primary and secondary contingencies could be impacted across multiple geographic locations; it placed an emphasis on capacity and sustainability planning within teams (e.g. resulting from illness and caring responsibilities) in contingency settings. It also altered the resource mix that underpins the delivery of services in BAU and Contingencies e.g. increase reliance on technology to support remote working or by accelerating the use of digital first services, whilst also altering the contingencies e.g. with some firms standing down or reducing traditional contingencies e.g. the use of alternative premises (Workarea recovery).

Space Weather	Scenario Category
	Natural Hazards & Public Health

Scenario Description	
Overview	This scenario explores a 1/100 plus severe, but plausible, space weather event that results in impacts to global communications and navigation systems, energy and transportation infrastructure and financial markets.
Cause	A solar maximum (Carrington-class[2]) event sees the largest solar storm since 1859 impact earth's atmosphere with the level of impact exceeding anything previously experienced due to every increase and pervasive dependency of technology systems in particular space-based system.
Impact (Incl. Scale)	• Space weather monitoring agencies observe a series of intense solar flares from a complex, growing group of active sunspots. They issue a space weather alert for strong coronal mass ejections (CMEs) - powerful eruptions of magnetic fields and plasma which travel through space and affect Earth. The affected region/s are alerted to prepare for disruption within 15 – 24hrs. • Upon arrival, and despite built in mitigations, the CME causes unprecedented damage to global satellite systems [insert %], communications, energy, and transport infrastructure with disruption expected to be measured in days (for satellite-based systems) and weeks where repairs will take longer e.g. to power infrastructure. • The CME causes regional and localised power outages both directly (e.g. damaged power infrastructure such as transformers) and through controlled shutdowns designed to limit the damage and protect higher risk sites. • There is widespread unavailability of public and commercial transportation (due to the impact on satellite navigation-based systems), and a range of public services including schools are closed. • Impacts are further compounded by reports of widespread disruption to internet-based services resulting from the impact to the electrical power required to drive optical repeaters distributed along undersea cables which are supplied by long conducting wires running alongside the fibres. These wires are vulnerable to geomagnetically induced currents (GICs). • For these reasons [xx%] of staff are assessed as unable to either travel to and/or work from home due to an either or a combination of power, connectivity or caring responsibilities. • Although the impact to commercial mobile telephony is limited (as the UK commercial network is not reliant on impacted Global Navigation Satellite System (GNSS)), there is still some disruption resulting from damage to power outages and hardware failures. • The extent of damage to ground-based infrastructure is unclear but solar energetic particles indirectly generate charge in semiconductor materials, causing electronic equipment to malfunction. [SV: There are reports of Data Centres going offline due to power and technology infrastructure failures] • Although [for some], there are contingency options and redundancy built within firm's internal timing infrastructure, the loss of access to satellite alignment, if extended over a period of [xx] days, would create significant operational challenges. The financial services firms that are required to meet the Markets in Financial Instruments Directive (MiFID II) requirements on the synchronisation of business clocks3 would be most impacted. The importance of synchronised timing is primarily around trading where the granularity of

	timing, and the accuracy of event sequencing is significant for regulatory transaction reporting. [SV: As a result of multiple market participants reporting challenges in their ability to maintain accurate transaction time, trading is suspended in certain markets] • Critical third parties supporting FS are equally impacted and there are widespread upstream impacts to supply chains through the disruption to commercial transportation resulting from the impact to GNSS. • Emergency services, despite mitigations, are hampered by disruption to emergency communications (which does depend on GNSS), impeding their response to outbreaks of civil unrest and elevated criminal activity seeking to exploit the situation.

[Risk] Coverage	People ☒	Property ☒	Technology ☐	Data (Availability) ☒	Data (Integrity) ☒	Third Party ☒

Characteristics	• **Rapid onset** - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place. Solar flares can take as little as 8 mins to reach earth although CME, the type of which are more widely associated with broader based disruption typically have 15-24hrs notice. • **Disrupted Communication** - Internal and external communication channels are impaired by the nature of the incident. • **Elevated Staff anxiety** - resulting from actual or perceived threat to safety of staff and/or family members and concerns over firm stability. • **Conflicting priorities** - During incidents with potential broader societal impacts, staff may face competing prioritise regarding family/caring responsibility, limiting their ability to work/support the firms response. • **Pan regional** impacts may limit use of transference strategies.
Assumptions	• Incident happens at peak and/ or significant trading day with above average volume.

Stress variables *(illustrative levels, to be adjusted as appropriate)*

Impact Radius	UK ☐	EMEA ☐	APAC ☐	Americas ☐	Global ☐
Impact to internet	Yes (latency) ☐	Yes (loss of connectivity) ☐	- ☐	- ☐	- ☐
Impact to Data Centres	No ☐	Single ☐	Multiple ☐	- ☐	- ☐
Markets	Open ☐	Closed (1day) ☐	Closed (2 days) ☐	Closed (3 days) ☐	- ☐

Case Study	
Causation/ Impact (Risk Coverage):	In 1989, a series of geomagnetic storms (coronal mass ejections) stuck earth in March, August and October resulting in instances of wide area power loss, the unavailability of technology (land and space-based systems) and disruption to financial markets.

Impact (scale):	The March 1989 event caused blackouts across a number of areas including in Quebec which left the whole province without power impacting [9 million] people after the Hydroelectric power system went offline. In Aug 1989, the Toronto stock market halted trading after another large storm caused damage to [microchips].
Duration:	As seen in 1989, space weather events can be single or multiple events over a series of time, like non-space weather events. Depending on the intensity of the event, the impact to systems will vary. In March 1989 power was lost to the Quebec region for 9 hours and in the Oct 1989 storms, the Toronto stock exchange closed for several hours.
Compound Scenario Considerations:	By default, a severe space whether event would impact multiple resource types from power, technology and broader society as both staff and customers contend with disruptions to essential services including power and transportation and the resultant impact that would have on other services such as emergency services, schools, hospitals etc.
Takeaways:	It is hard to ascertain how impactful an extreme space weather event would be – improvements in the engineering of systems to withstand space weather events (e.g. the use of holdovers and land-based connections to atomic closes) has improved but reliance on technology, including satellite-based technology has increased significantly since some of the most well-known incidents involving space weather. A 'Carrington' level space weather event could be far more impactful in scope and duration of the impacts seen in 1989 and more recently. Although lower probability, firms should consider the potential impacts to power, technology infrastructure (land and space based) on their operations and to their staff based on broader impacts to society where essential services are impacted.

Critical National Infrastructure

Localised Loss of Power						**Scenario Category**
						CNI
Scenario Description						
Overview	This scenario explores a regional power outage for a prolonged period, resulting in an impact to buildings and people working from home.					
Cause	Physical Infrastructure Issue leading to Regional Power Failure.					

Impact (Incl. Scale)	• The regional power outage is caused by a technical issue and spans a [20 mile] radius from [firms] main office and there has been no notice of the event to preplan. There is uncertainty of the length of time it will take to restore services, but they have indicated it will be [several days]. There is an expectation on restoration of power there will be a couple of days with intermittent power issues. The general public have been advised to not travel unless critical.
	• Although the scenario assumes you will have UPS/generators, access to the internet will be unavailable and therefore you cannot reach your data centres to continue to provide a service. Power outages will impact water in the region so all offices will have to close for Health & Safety purposes. You will have limited/no communication channels to the staff impacted during the outage.
	• A regional power outage will increase the anxiety of your staff.
	  ○ People not impacted will be worrying about their colleagues during the outage and performance may be impacted.
	  ○ On recovery, the staff impacted could have increased levels of anxiety/stress and as a result there may be increased sickness levels.
	• As this scenario is regional then not all customers will be impacted and there will be an expectation to continue to provide a service.					

[Risk] Coverage	People ☒	Property ☒	Technology ☒	Data (Availability) ☒	Data (Integrity) ☐	Third Party ☒
Characteristics	• **Rapid onset** - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place. • **Disrupted Communication** - Internal and external communication channels are impaired by the nature of the incident. • **Elevated Staff anxiety** - resulting from actual or perceived threat to safety of staff and/or family members and concerns over firm stability. • **Conflicting priorities** - During incidents with potential broader societal impacts, staff may face competing prioritise regarding family/caring responsibility, limiting their ability to work/support the firms response.					
Assumptions	• Incident happens ahead of peak and/ or significant trading day with above average volume. • Power outage happens during the working day. • UPS/Generators will work as expected to facilitate shutdowns and evacuations.					
Stress variables *(illustrative levels, to be adjusted as appropriate)*						
Expansion of radius	50 miles ☐	75 miles ☐	100 miles ☐	150 miles ☐	200 miles ☐	

Third Parties Impacted	No ☐	Yes ☐	-	-	-
Increase outage time	2 days ☐	3 days ☐	4 days ☐	7 days ☐	10 days ☐
Data Centres	No ☐	Yes ☐	-	-	-
Case Study					
Causation/ Impact (Risk Coverage):	In January 2025 Storm Éowyn wreaked havoc on electricity and telecoms infrastructure. With record wind gusts exceeding 180 km/h recorded in Ireland and a 'major incident' declared on the Isle of Man, the storm has been historic in both its strength and the extent of the damage caused across the islands.				
Impact (scale):	Ireland's state electricity supplier, ESB Networks, reported "unprecedented" power outages impacting over 725,000 premises (equivalent to as much as one-third of all homes in the country). The extensive damage to the electricity grid has had severe knock-on effects on both fixed and mobile network infrastructure, with well over a thousand mobile sites taken offline due to disruptions to mains power and downed trees causing damage to overhead fibre cabling along roads.				
Duration:	Restoration times expected to exceed a week in the hardest-hit areas				
Compound Scenario Considerations:	Storm Éowyn was a red weather warning for Ireland with schools and shops being closed and people not being allowed to travel. This resulted in the resilience of powers in office buildings could not be utilised by anyone who had no power at home. As well as impacting power across the country mobile communication was severely impacted				
Takeaways:	As a result of climate change storms like Storm Éowyn could become more frequent and become more extreme resulting in wider power outages lasting longer.				

National Power Outage (NPO)						Scenario Category
						CNI
Scenario Description						
Overview	This scenario explores a national power outage for a prolonged period, resulting in a complete failure of both power and telecoms, leading to a cascading failure of water, sewerage, transport services across the country.					
Cause	Physical or Network Infrastructure Damage Issue leading to National Power Outage.					
Impact (Incl. Scale)	• The national power outage is caused by a technical issue and spans the entire country. There has been no notice of the event to preplan. There is uncertainty of the length of time it will take to restore services, but they have indicated it will be up to 7 days. There is an expectation on restoration of power there will be a couple of days with intermittent power issues. The general public have been advised to not travel unless critical. • The only communications channel available is the BBC Emergency Service (one-way government messaging). • Although the scenario assumes you will have UPS/generators, access to the internet will be unavailable and therefore you cannot reach your data centres to continue to provide a service. • Health & Safety issues will exist whether you expect to keep staff on premises or attempt to send them home. You will have limited/no communication channels to the staff impacted during the outage. • A regional power outage will increase the anxiety of your staff.					
[Risk] Coverage	People ☒	Property ☒	Technology ☒	Data (Availability) ☒	Data (Integrity) ☐	Third Party ☒
Characteristics	• **Rapid onset** - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place. • **Disrupted Communication** - Internal and external communication channels are impaired by the nature of the incident. • **Elevated Staff anxiety** - resulting from actual or perceived threat to safety of staff and/or family members and concerns over firm stability. • **Conflicting priorities** - During incidents with potential broader societal impacts, staff may face competing prioritise regarding family/caring responsibility, limiting their ability to work/support the firms response.					
Assumptions	• Incident happens ahead of peak and/ or significant trading day with above average volume. • Power outage happens during the working day. • UPS/Generators will work as expected to facilitate shutdowns and evacuations.					
Stress variables *(illustrative levels, to be adjusted as appropriate)*						
Increase outage time	2 days ☐	3 days ☐	4 days ☐	7 days ☐	10 days ☐	
Civil Unrest	5% ☐	15% ☐	25% ☐	75% ☐	Complete Societal Breakdown ☐	

Sickness levels following power recovery	5% ☐	15% ☐	25% ☐	75% ☐	95% ☐
Case Study					
Causation/ Impact (Risk Coverage):	On 29 October 2012 Superstorm Sandy made landfall near Atlantic City, NJ. In addition to the loss of lives and property, Sandy caused billions of dollars of damages to homes, underground infrastructure and power lines. It caused broad based impact across all resource types e.g. premise, people, technology and third parties.				
Impact (scale):	In addition to the direct loss of life, Sandy shut down or damaged at least 165 electric substations, several large power plants, 7,000 transformers, and 15,000 electrical poles. More than 8 million people in 21 states were without power. Sandy caused widespread disruption to transport infrastructure. In terms of Financial Services, the NYSE and Nasdaq were closed for 2 days, with telecom disruption impacting trading. Some firms sustained significant damage to their premise including Data Centres, impacting re-opening[8].				
Duration:	The NYSE re-opened following a 2-day closure, however, some firms continued to experience disruption to their operations as power restoration ranged from days to weeks across the states.				
Compound Scenario Considerations:	This scenario highlights that power outages often represent only one impact type resulting from events such as severe weather. For many firms, the principal impacts were to their people and premises, but for others this extended to technology and their supply chain.				
Takeaways:	Sandy highlighted that although power/building resilience can be engineered for a firm's premises, if wider power and transportation disruption occurs, these locations may be inaccessible for staff reliant on public or private transportation. Likewise, the widespread power loss highlights the potential limitations of a pure WFH contingency strategy and broader societal impact may result in elevated staff absence where other public services such as schools are closed. As a result of climate change severe weather events could become more frequent and become more extreme resulting in wider and more impactful power outages.				

[8] Aon Benfield, 2014, cited in Disaster Recovery Case Studies. US Storms 2021: Super Storm Sandy https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-case-study-superstorm-sandy.pdf

Third Party

Loss of Cloud Service Provider (CSP)						**Scenario Category** Third Party
Scenario Description						
Overview	This scenario explores the unavailability of a CSP supporting multiple Firms across Financial Services, resulting in business, operational and consumer impacts.					
Cause	A [poorly executed change/software bug/cyber-attack] leads to a high profile CSP being unable to deliver services across multiple availability zones within a region for a prolong period.					
Impact (Incl. Scale)	• The outage has impacted firms that rely on the CSP for the hosting of a range of critical services supporting IBS including infrastructure supporting firms' core [banking/insurance] platform(s). • The CSP struggles to identify the root cause and is therefore unable to estimate when services will be resumed. • Recovery from a [cold] back-up arrangement to another region has not been possible, although it is unclear whether this is the same or unconnected issue. • Services remain unavailable at the end of day. As such, impacted firms are unable to carry key end of day activities e.g. key deadlines on payments and reporting have been missed. • Eventually the underlying issue is identified, and recovery commenced with the aim of completing all end of day processes and a full recovery by start of the next business day. However, the recovery was only partially successful as the firm is unable to fully reconcile the balances and it will require up to 1600hrs on Day 2 before all services can be. • All IBSs reliant on services provided by the CSP including the core [banking] platform are impacted / all digital channels are also disrupted, and IBSs are not available to end-users. • As the affected CSP is a market leading company, there is a risk broad impact to the market as multiple Financial Institutions are impacted. • The high-profile nature of the CSP results in extensive media coverage of the difficulties caused to clients which dominates regional and international news cycles.					
[Risk] Coverage	People ☐	Property ☐	Technology ☒	Data (Availability) ☒	Data (Integrity) ☒	Third Party ☒
Characteristics	• **Rapid onset** - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place. • **Low predictability / highly changeable** due to uncertainty as to cause. • **Uncertain duration** of investigation, containment and technical recovery time makes estimating business recovery times difficult. • **Higher scrutiny** and potential to undermine stakeholder trust - through perceived or actual lack of action/transparency due to nature of incident. • **Other:** Elevated market/regulator concern due to potential for market impact.					

Assumptions	• Incident happens on a peak and/or significant trading day with above average volume (in line with the worst-case scenario used for setting impact tolerance).				
Stress variables *(illustrative levels, to be adjusted as appropriate)*					
Duration of CSP issue	24hrs / NBD ☐	36 - 48 hours ☐	48 - 72hrs ☐	72 – 96 hrs ☐	>1week ☐
Third Party Service Impact	<25% ☐	25 - 50% ☐	50% ☐	50% - 75% ☐	Stressed exit ☐
Case Study					
Causation/ Impact (Risk Coverage):	On 25APR23 water leaked from a non-Google room, into a Google Cloud Platform (GCP) data centre within its europe-west9 region (located in Paris), leading to a fire in an associated Unlimited Power Supply (UPS) room and subsequent evacuation and power shutdown of the data centre (Europe-west9-a).				
Impact (scale):	Although the three data centres (a,b,c) within the region run on separate infrastructure, the incident had a regional impact due to a misconfiguration of the regional spanner (backend database) used by several GCP services which had two of its three replicas in two clusters within the impacted DC (instead of in each building). Google advised that Clients reliant on the impacted services could fail over to zones in other regions.				
Duration:	The incident resulted in the regional unavailability of multiple services on 25-26APR25 with some services impacted for an extended period beyond that.				
Compound Scenario Considerations:	This scenario highlights the interplay between the unavailability of premise and a misconfiguration of a back-end data base which meant that data centres designed to be independently resilient to a power outage (by running on separate infrastructure) where all impacted by same incident.				
Takeaways:	Although cloud hosted services may offer potential benefits to resilience vs traditional on-premise solutions, this incident, along with other examples across different suppliers, highlights that even systems designed to be highly resilience can be subject to failures which cause extended outage of services reliant upon them.				

Loss of a Financial Market Infrastructure (FMI)	**Scenario Category**
	Third Party

Scenario Description						
Overview	This Scenario explores the loss of a critical FMI supporting Firms across Financial Services, resulting in business, operational and consumer impacts.					
Cause	A [poorly executed change/cyber-attack/technology failure] leads to a critical FMI being unable to service Firms domestically and internationally for an undisclosed period of time.					
Impact (Incl. Scale)	• The disruption has impacted all firms that rely on that FMI for supporting their Important Business Services (IBS). • During the initial stages of the incident, the FMI is unable to provide a root cause of the incident and therefore is unable to estimate when services will be resumed. • It appears that services being provided by other FMIs within the sector are unaffected by the disruption to the FMI, however, should there be dependencies on that FMI, it may lead to secondary impacts. • Services being provided by the FMI remain unavailable at the end of the day, leading to potential issues for firms end of day activities and potential knock-on impact on other firms and customers. • The FMI is unable to failover initially to a secondary site as the root cause is not confirmed so cannot guarantee that there will not be the same issues after failing over. • Due to the interdependency across the sector on the FMI, there are potentially significant financial penalties that multiple firms may be facing should they not be able to fulfil their services by the following working day. • During the night the FMI is able to identify the root cause of the issue and provides an update to clients that this will take a number of hours to recover, which may not just impact the ability to complete end of day processes, but also start of day activities as well. • Recovery activities take longer than initially expected and some organisations are identifying gaps within their data sets from the FMI. • CMBCG has been running since the initial disruption as has Authorities Response Framework (ARF) due to the criticality of the FMI and the potential fear that this may lead to greater market disruption. • Media coverage has been building over the previous day and in the morning as IBSs are breaching ITOLs and customers are beginning to feel the impact of the disruption. • The FMI is able to fully recover in time for that day's end of day activities and begins the processes of catching up on the previous day's activities in time for BAU opening the following working day.					
[Risk] Coverage	People ☐	Property ☐	Technology ☒	Data (Availability) ☒	Data (Integrity) ☒	Third Party ☒
Characteristics	• **Rapid onset** - this is a no-notice or minimal notice event with little to no time to put additional mitigations in place. • **Low predictability / highly changeable** due to uncertainty as to cause.					

	• **Uncertain duration** of investigation, containment and technical recovery time makes estimating business recovery times difficult. • **Higher scrutiny** and potential to undermine stakeholder trust - through perceived or actual lack of action/transparency due to nature of incident. • **Other:** Elevated market/regulator concern due to potential for market impact.				
Assumptions	• Incident happens on a peak and/or significant trading day with above average volume (in line with the worst-case scenario used for setting impact tolerance). • No initial timeframe is provided by the FMI on when the incident will be resolved.				
Stress variables *(illustrative levels, to be adjusted as appropriate)*					
Duration of disruption	<24hrs ☐	24 - 48 hours ☐	48 - 72hrs ☐	72 – 96 hrs ☐	>1week ☐
IBS Impacted	<20% ☐	20-40% ☐	40-60% ☐	60-80% ☐	>80% ☐

Note: There is currently no case study for the loss of an FMI scenario.

Annex A. Template and guidance for populating / reading a scenario.

The following section shows the format for the scenarios within the DSL with accompanying guidance for how each section is/should be completed.

<table>
<tr><td colspan="6">[Scenario Name]</td><td>Scenario Category
[Insert]</td></tr>
<tr><td colspan="7">Scenario Description</td></tr>
<tr><td>Overview</td><td colspan="6">This section provides a high-level summary of the scenario. The remainder of the scenario description should flow as a single narrative, starting with the cause, then how the scenario impacts a firm(s) in terms of type and nature of the resources impacted along with number of IBS likely to be impacted.</td></tr>
<tr><td>Cause</td><td colspan="6">This section outlines the cause of the disruption and may include both an initiating event / trigger and a vulnerability which allows the trigger event to impact the firm e.g. a weakness in the control environment. For security related events, this will also include the threat actor and their motivation.</td></tr>
<tr><td>Impact
(Incl. Scale)</td><td colspan="6">This section represents the ‘base scenario’ and should cover:
• The narrative description of how the impact is manifest – the onset and any transmission and amplification through which of the resources that underpin the operational delivery of the firms IBS.
• The section may include elements of the initial response where appropriate in order to move the storyline to an appropriate point in time from which to start the test. For example, a pandemic scenario will typically consider the response and recovery at a time further along from when the first case was identified. NB: this does not remove the requirement for firms to still consider detective and containment controls.
• Finally, the scenario should provide an indicative sense of the scale of the scenario impact in terms of the number of IBS impacted, although specificity will be limited to allow for the broadest use of the scenario.
• For parts of the scenario that related to stress variables that can be adjusted to alter severity, reference to the stress variables table is indicated with (SV)</td></tr>
<tr><td>[Risk] Coverage</td><td>People
☒</td><td>Property
☒</td><td>Technology
☒</td><td>Data (Availability)
☐</td><td>Data (Integrity)
☐</td><td>Third Party
☒</td></tr>
<tr><td>Characteristics</td><td colspan="6">• The scenario characteristics provides context around the nature of the scenario being tested and how that may affect the need for and/or the effectiveness of certain recovery action.
• Is there a particular 'quality' of the scenario that may necessitate additional response and recovery actions or alter the level of certainty within the scenario.
• See Appendix [x] for a summary of scenario characteristics included within the DSL</td></tr>
<tr><td>Assumptions</td><td colspan="6">This section outlines and key assumption(s) upon which the response and recovery to the scenario should considered. They can be used to help isolate the variables being tested and set the parameters around the test by ensuring common understanding of the basis on which decisions are made. Examples could include statements around the availability or the ability to contact staff key to executing recovery actions in scenario not focused primarily on loss of staff i.e. where this wouldn’t be covered in the scenario description.</td></tr>
</table>

Stress variables *(illustrative levels, to be adjusted as appropriate)*
The stress variable section of the scenario can be used either an 'options list' for increasing the severity of the base scenario or for the different stages within a stress test scenario format where the variables are used 'ratchet up' the severity of a scenario from its 'base scenario' in order to identify the point in which impact tolerance would be breached. Each scenario should ideally contain between 3 and 5 scenario variable categories and levels of severity. Although options are provided firms can alter as required. In addition, to the variable outlined in each scenario, please also refer to Appendix [x] Causation to Impact Mapping which can be used to scale the impact by moving along the impact options based on the scenario cause.

NB: aspects of the scenario scale such as number of IBS impacted are not included and should be incorporated as part of the localisation of the base scenario. Stress Variable Examples below:

Staff Absence	20% ☐	35% ☐	50% ☐	75% ☐	100% ☐
Duration of lockdowns /	2-4 weeks ☐	4-8 weeks ☐	8-12 weeks ☐	6 months ☐	1 year ☐
Third Party Service Impact	<25% ☐	25 - 50% ☐	50% ☐	50% - 75% ☐	Stressed exit ☐

Case Studies – The purpose of a case study is to bring the scenario to life and demonstrate plausibility through historical precedence. Case studies can be an effective mechanism to persuade sceptical participants who may have never heard of such a scenario being experienced by others before. Case studies should typically, be 3-5 sentences in length, drawn from open source and easily referenced without using links.

The scenario should cover.

- An overview of the incident, demonstrating relevance and supporting scenario plausibility by highlighting historical precedence for the scenario by giving a real live example of the cause of the disruption or the nature of the impact.
- The key takeaways that emphasise aspects of the scenario e.g. the risk coverage, severity, characteristics.
- Where possible feature impacts to the financial services sector.
- Avoid speculative commentary where causation has not been established.

Although some case studies include links to sources and/or reference material, where citing any case studies from the DSL, it is the responsibility of the firm doing so to validate any numbers/statements included within them.

An example is provided below:

Causation/ Impact (Risk Coverage):	On 19JUL24, CrowdStrike, a third-party cybersecurity company, distributed a faulty update following a poorly executed change, to its Falcon Sensor security (vulnerability scanning) software resulting in widespread unavailability of technology (principally those running MS Operating Systems)
Impact (scale):	Approximately 8.5 million systems were impacted across multiple sectors, including financial services, disrupting both the private sector and public sector organisation and services including transportation.

Duration:	Although the error was discovered and a fix released within hours, many computers required manual interventions prolonging the outage for some services over several days.
Compound Scenario Considerations:	For some organisations in the US, the impact from the CrowdStrike change compounded the impact from the previous days disruption to MS Azure Cloud Services impacting MS365 and other services.
Takeaways:	The incident highlighted the potential for disruption caused by third party software updates to impact a firm and other third parties they rely on, meaning firms need to consider simultaneous internal disruption and disruption to one or more 3rd parties. It also highlighted potential shortfalls with robustness of a firms own controls to manage sources of disruption from third Party software providers and in certain circumstances, the challenge of high-volume manual interventions which raises questions over firms' ability to mobilise the required (skilled) resources to execute a timely recovery.

References & Useful Resources: The following section should be used for any sources / references that underpin the scenario e.g. where a % of staff absence is linked to a National Risk Register

Suggested capture of changes to the base scenario. NB: this can but does not have to include stress variables as these are designed to be selected by the individual firm.

Localisation		
Section	**Part of base scenario changed**	**Rationale**
Scenario Description		
Characteristics		
Assumptions		

Annex B. Scenario Causation to Impact Mapping

The table below shows Scenario 'causation' to 'impact' mapping, indicating the principal relationship between the scenario cause and how that may manifest in an impact(s) to aspects of a firm's technology, data, premises, people and third parties. For simplicity it does not include all secondary relationships or every possible link through chains of impact. However, these should not be discounted when adapting or scaling (severity) of scenarios from the DSL. For example, human error can be a cause in its own right or the reason for a poorly executed change becoming a disruption. Likewise severe weather events can lead to 'unavailability of power and utilities' that can then lead to the unavailability of colleagues who are unable to travel into work or work from home. When using this mapping, firms should localise in line with the organisational and technology architecture of their respective firms.

			Unavailability of Technology								Unavailability of Data			Unavailability of Buildings (Non-Tech)			Unavailability of People		Unavailability of Third Party		
Category	Ref	DSL Scenario (Causation)	Unavailability of an application	Unavailability of multiple applications	Complete unavailability of a data centre or Cloud Availability Zone All workloads within a DC / AZ are unavailable	Loss of multiple or all DCs / AZ within a region	Global loss of CSP services e.g. Relational DBMS	Unavailability of application (production and DR resulting from a cyber-attack)	Unavailability of Core Technology	Disruption to fixed and/or mobile and telecommunications	Sudden Unavailability of data availability	Data is inconsistent, inaccurate or incomplete - Single Application	Data is inconsistent, inaccurate or incomplete across connected applications / within one or more IT Service	Unavailability of building*	Unavailability of multiple buildings e.g. Campus Wide / City	Unavailability of multiple buildings (Country Wide).	Unavailability of individual (SPOF)	Unavailability of multiple colleagues	Unavailability of Material Third Party (Inc. CSP)	Unavailability of an FMI	Unavailability of a G-SIB or G-SFI
1. Technology & Data (Cyber)	1.1	Cyber Attack - Malware e.g. Ransomware	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y						Y	Y	Y
	1.2	Cyber Attack - Distributed Denial of Service	Y	Y	Y	Y			Y	Y	Y								Y	Y	Y
	1.3	Generative AI - Staff Account Creation							Y			Y	Y				Y	Y	Y		
	1.4	Generative AI - Customer Account Creation							Y			Y	Y						Y		
2. Technology & Data (Non-Cyber)	2.1	Poorly Executed Change	Y	Y	P [Network Change]	Y	Y		Y	Y	Y	Y	Y	Y					Y	Y	Y
	2.2	Hardware/Software Failure	Y	Y	P [Building infra]				Y	Y	Y	Y	Y	Y					Y	Y	Y
	2.3	Procedure/Human Error	Y	Y	Y				Y	Y	Y	Y	Y	Y					Y	Y	Y
3. Physical Security	3.1	Terrorism - Mass Destruction												Y	Y		Y	Y	Y	Y	Y
	3.2	Terrorism - Marauding Armed Intruders												Y	Y		Y	Y	Y	Y	Y
	3.3	CBRN Attacks												Y	Y		Y	Y	Y	Y	Y
4. Geopolitical	4.1	Civil Unrest												Y	Y	Y	Y	Y	Y	Y	Y
	4.2	Intrastate Conflict												Y	Y	Y	Y	Y	Y	Y	Y
	4.3	Regional Conflict												Y	Y	Y	Y	Y	Y	Y	Y
	4.4	Disruption to Undersea Cables	Y	Y	Y	Y			Y	Y	Y								Y	Y	Y

Scenario Causation to Impact Mapping Continued

			Unavailability of Technology								Unavailability of Data			Unavailability of Buildings (Non-Tech)			Unavailability of People		Unavailability of Third Party		
Category	Ref	DSL Scenario (Causation)	Unavailability of an application	Unavailability of multiple applications	Complete unavailability of a data centre or Cloud Availability Zone All workloads within a DC / AZ are unavailable	Loss of multiple or all DCs / AZ within a region	Global loss of CSP services e.g. Relational DBMS	Unavailability of application (production and DR resulting from a cyber-attack)	Unavailability of Core Technology	Disruption to fixed and/or mobile and telecommunications	Sudden Unavailability of data availability	Data is inconsistent, inaccurate or incomplete - Single Application	Data is inconsistent, inaccurate or incomplete across connected applications / within one or more IT Service	Unavailability of building*	Unavailability of multiple buildings e.g. Campus Wide / City	Unavailability of multiple buildings (Country Wide).	Unavailability of individual (SPOF)	Unavailability of multiple colleagues	Unavailability of Material Third Party (Inc. CSP)	Unavailability of an FMI	Unavailability of a G-SIB or G-SFI
5. Industrial Accidents	5.1	Major Industrial Accidents (Nuclear)													Y	Y	Y	Y	Y	Y	Y
	5.2	Major Industrial Accidents (Non-Nuclear)													Y	Y		Y	Y	Y	Y
6. Natural Hazards & Public Health	6.1	Severe Weather (e.g. Hurricanes/Storms)								Y				Y	Y	Y	Y	Y	Y	Y	Y
	6.2	Non-weather geo-hazards (Earthquake / Volcanic)								Y				Y	Y		Y	Y	Y	Y	Y
	6.3	Severe Contagious Disease e.g. Pandemic												Y	Y	Y	Y	Y	Y	Y	Y
	6.4	Severe Space Weather	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
7. Critical National Infrastructure	7.1	Localised Loss of Power	Y	Y	Y	Y			Y	Y	Y			Y	Y	Y		Y	Y	Y	Y
	7.2	National Power Outage (NPO)	Y	Y	Y	Y			Y	Y	Y			Y	Y	Y		Y	Y	Y	Y
	7.3	Unavailability of Telecoms / Network Infrastructure	Y	Y	Y	Y			Y	Y											
8. Third Party	8.1	Unavailability of Material Third Party (Inc. CSP)	Y	Y	Y	Y	Y	Y	Y										Y	P	P
	8.2	Unavailability of an FMI																		Y	
	8.3	Unavailability of a G-SIB or G-SFI																			Y

Key: Y (Yes); N (No); P (Potentially)

Annex C. Standardised list of Scenario Characteristics

The following table shows suggested scenario characteristics for each scenario contained within the DSL.

Characteristic	Characteristic (Sub Cat)	Description and Considerations when designing a scenario test	Cyber - Malware	Cyber via Supply Chain Attack	Staff Account Creation	Customer Account Creation	Poorly Executed Change	Terrorism - Mass Destruction	Terrorism - Marauding Armed Intruders
Speed of onset (Lead time)	Slow onset and/or Chronic	• Longer lead time provide potential for pre onset actions. • Chronic by nature placing a greater emphasis on sustainability of recovery strategies.							
	Rapid / Acute (Little to no lead time)	• This is a no-notice or minimal notice event including Zero Hr attack • Little to no time to put additional mitigations in place • Immediacy and pace of disruption places a greater emphasis on effective detection well documented and rehearsed immediate actions e.g. containment and mitigating response.	Y	Y	Y	Y	Y	Y	Y
Level of changeability & persistence	Low predictability / highly changeable (Threat Actor)	The defining characteristic of these scenarios is that the 'enemy gets a vote' or in other words there are moves and countermoves that make the end-to-end response and recovery, from detection to restoration hard to predict, cause persistence in the disruption and will likely cause protracted timeframes and firms take measures to reassure themselves and others that the threat has been contained and/or eliminated.	Y	Y	Y	Y	Y	Y	Y
	High persistence	Scenarios with high persistence are characterised with recurring periods of disruption although each period may vary in nature, scale and duration. Examples may include technology outages where service become available only to then experience performance degradation and further periods of downtime. This may also be the case with cyber related scenarios where a threat actor adapts their behaviour and tactics in response the firm counter measures.	Y	Y		Y			
Information asymmetry & communication	Information asymmetry	Scenarios that are characterised as typically having high information asymmetry are those where a firm's ability to directly obtain, gather or analysis information relevant to their response and recovery is limited, resulting in decision making on incomplete or inaccurate information/intelligence. For example, the motivations of a threat actor may be unknown or the true severity of a disruption to a third party may not be fully visible.	Y	Y	Y	Y		Y	Y
	Disrupted Communication	Some scenarios by their very nature may disrupt the means through which firms communicate in both BAU and in their response. The most obvious examples are cyber related which may render company supported devises unusable removing the means to communicate securely. Other scenario my temperately disrupt communications through physical damage to infrastructure.	Y	Y	Y			Y	Y
Emphasis on Customer trust, Staff anxiety and conflicting priorities	Higher scrutiny and potential to undermine stakeholder trust	Higher scrutiny and potential to undermine stakeholder trust - through perceived or actual lack of action/transparency due to nature of incident.	Y	Y	Y	Y	Y		
	Staff anxiety	All crisis, disasters or severe disruptions cause some form of anxiety but those scenarios where this is a defining characteristic are those where the nature and trajectory of the disruption is unknown and/or where there are direct safety implications to staff and their families.			Y	Y		Y	Y
	Conflicting priorities	Security based and wide area events like acts of terror or geohazards will often mean staff have the safety and needs of their families to address, limiting their ability to support the firm's response. Staff may behave unpredictably or be contactable or unavailable. Planning needs to consider the implication around levels of staff availability, burn out and other factors.							

Scenario Characteristics Continued (Scenarios 3.1- 6.3):

Characteristic	Characteristic (Sub Cat)	Description and Considerations when designing a scenario test	Civil Unrest	Disruption to Undersea Cables	Severe Weather	Global Pandemic	Space Weather	Localised Loss of Power	National Power Outage (NPO)
Speed of onset (Lead time)	Slow onset and/or Chronic	• Longer lead time provide potential for pre onset actions. • Chronic by nature placing a greater emphasis on sustainability of recovery strategies.	Y		Y	Y			
	Rapid / Acute (Little to no lead time)	• This is a no-notice or minimal notice event including Zero Hr attack • Little to no time to put additional mitigations in place • Immediacy and pace of disruption places a greater emphasis on effective detection well documented and rehearsed immediate actions e.g. containment and mitigating response.		Y			Y	Y	Y
Level of changeability & persistence	Low predictability / highly changeable (Threat Actor)	The defining characteristic of these scenarios is that the 'enemy gets a vote' or in other words there are moves and countermoves that make the end-to-end response and recovery, from detection to restoration hard to predict, cause persistence in the disruption and will likely cause protracted timeframes and firms take measures to reassure themselves and others that the threat has been contained and/or eliminated.	Y			Y			
	High persistence	Scenarios with high persistence are characterised with recurring periods of disruption although each period may vary in nature, scale and duration. Examples may include technology outages where service become available only to then experience performance degradation and further periods of downtime. This may also be the case with cyber related scenarios where a threat actor adapts their behaviour and tactics in response the firm counter measures.	Y	Y		Y			
Information asymmetry & communication	Information asymmetry	Scenarios that are characterised as typically having high information asymmetry are those where a firm's ability to directly obtain, gather or analysis information relevant to their response and recovery is limited, resulting in decision making on incomplete or inaccurate information/intelligence. For example, the motivations of a threat actor may be unknown or the true severity of a disruption to a third party may not be fully visible.		Y					
	Disrupted Communication	Some scenarios by their very nature may disrupt the means through which firms communicate in both BAU and in their response. The most obvious examples are cyber related which may render company supported devises unusable removing the means to communicate securely. Other scenario my temperately disrupt communications through physical damage to infrastructure.		Y	Y		Y	Y	Y
Emphasis on Customer trust, Staff anxiety and conflicting priorities	Higher scrutiny and potential to undermine stakeholder trust	Higher scrutiny and potential to undermine stakeholder trust - through perceived or actual lack of action/transparency due to nature of incident.							
	Staff anxiety	All crisis, disasters or severe disruptions cause some form of anxiety but those scenarios where this is a defining characteristic are those where the nature and trajectory of the disruption is unknown and/or where there are direct safety implications to staff and their families.	Y		Y	Y	Y	Y	Y
	Conflicting priorities	Security based and wide area events like acts of terror or geohazards will often mean staff have the safety and needs of their families to address, limiting their ability to support the firm's response. Staff may behave unpredictably or be contactable or unavailable. Planning needs to consider the implication around levels of staff availability, burn out and other factors.	Y		Y	Y	Y	Y	Y

Scenario Characteristics Continued (Scenarios 6.4 - 8.2):

Characteristic	Characteristic (Sub Cat)	Description and Considerations when designing a scenario test	Loss of Cloud Service Provider (CSP)	Loss of a FMI (FMI)
Speed of onset (Lead time)	Slow onset and/or Chronic	• Longer lead time provide potential for pre onset actions. • Chronic by nature placing a greater emphasis on sustainability of recovery strategies.		
	Rapid / Acute (Little to no lead time)	• This is a no-notice or minimal notice event including Zero Hr attack • Little to no time to put additional mitigations in place • Immediacy and pace of disruption places a greater emphasis on effective detection well documented and rehearsed immediate actions e.g. containment and mitigating response.	Y	Y
Level of changeability & persistence	Low predictability / highly changeable (Threat Actor)	The defining characteristic of these scenarios is that the 'enemy gets a vote' or in other words there are moves and countermoves that make the end-to-end response and recovery, from detection to restoration hard to predict, cause persistence in the disruption and will likely cause protracted timeframes and firms take measures to reassure themselves and others that the threat has been contained and/or eliminated.	Y	Y
	High persistence	Scenarios with high persistence are characterised with recurring periods of disruption although each period may vary in nature, scale and duration. Examples may include technology outages where service become available only to then experience performance degradation and further periods of downtime. This may also be the case with cyber related scenarios where a threat actor adapts their behaviour and tactics in response the firm counter measures.		
Information asymmetry & communication	Information asymmetry	Scenarios that are characterised as typically having high information asymmetry are those where a firm's ability to directly obtain, gather or analysis information relevant to their response and recovery is limited, resulting in decision making on incomplete or inaccurate information/intelligence. For example, the motivations of a threat actor may be unknown or the true severity of a disruption to a third party may not be fully visible.	Y	Y
	Disrupted Communication	Some scenarios by their very nature may disrupt the means through which firms communicate in both BAU and in their response. The most obvious examples are cyber related which may render company supported devises unusable removing the means to communicate securely. Other scenario my temperately disrupt communications through physical damage to infrastructure.		
Emphasis on Customer trust, Staff anxiety and conflicting priorities	Higher scrutiny and potential to undermine stakeholder trust	Higher scrutiny and potential to undermine stakeholder trust - through perceived or actual lack of action/transparency due to nature of incident.	Y	
	Staff anxiety	All crisis, disasters or severe disruptions cause some form of anxiety but those scenarios where this is a defining characteristic are those where the nature and trajectory of the disruption is unknown and/or where there are direct safety implications to staff and their families.		
	Conflicting priorities	Security based and wide area events like acts of terror or geohazards will often mean staff have the safety and needs of their families to address, limiting their ability to support the firm's response. Staff may behave unpredictably or be contactable or unavailable. Planning needs to consider the implication around levels of staff availability, burn out and other factors.		

Annex D: Abbreviations

BAU	Business As Usual
CCG	Cyber Co-ordination Group
CMORG	Cross Market Operational Resilience Group
PMO	Project Management Office
CBRN	Chemical, Biological, Radiological, Nuclear
CIOF	Chief Information Officer Forum
CRR	Capital Requirements Regulation
CSP	Cloud Service Provider
DORA	Digital Operational Resilience Act
DSL	Dynamic Scenario Library
FCA	Financial Conduct Authority
FMEA	Failure Modes and Effects Analysis
FMI	Financial Market Infrastructure
G-SIB	Global Systemically Import Bank
G-SFI	Global Systemically Important Financial Institution
IBS	Important Business Service
ICAAP	Internal Capital Adequacy Assessment Process
ITOL	Impact Tolerance
NPO	National Power Outage
ORCG	Operational Resilience Collaboration Group
PRA	Prudential Regulatory Authority
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SBP	Severe But Plausible
SEG	Sector Exercising Group
SME	Subject Matter Expert
SLA	Service Level Agreement
SPOF	Single Point of Failure
SRR	Strategic Risk Register
SV	Stress Variable
TPRG	Third Party Resilience Group
UPS	Unlimited Power Supply