



Strategic and Enterprise Risks from Loss of Position Navigation, and Timing Services

Executive Summary

Satellite derived Position, Navigation and Timing (PNT) has become an “invisible utility” underpinning UK banking, transport and almost all critical national infrastructure – yet UK government analysis itself warns that national awareness of this dependence is “out of step with our actual dependence upon it.” This report sets out the eight most strongly evidenced strategic risks to the UK arising from loss, jamming, spoofing or systemic failure of PNT services, and extends that national picture across two further lenses that existing UK PNT policy does not currently cover: the United Nations (UN) Sustainable Development Goals (SDGs), and the enterprise risk register facing an individual commercial business.

The national strategic risk picture. Eight risks, corroborated across UK, US, Australian, international, academic, World Economic Forum and insurance sources, are grouped into three priority tiers. Tier 1 – cascading CNI failure, severe macroeconomic disruption, and multi-modal transport failure, carries the broadest reach; a sustained UK Global Navigation Satellite System (GNSS¹) outage is estimated to cost from £1.42bn (24 hours) to £7.64bn (7 days), against £13.62bn of annual UK economic benefit. Tier 2 covers telecoms, digital infrastructure, and trusted-time failure, emergency services and energy-system risk; Tier 3 covers adversarial denial and space-weather catastrophe, the latter carrying a probability-weighted global loss estimate of \$2.4 trillion over five years. Real-world interference is no longer theoretical, an estimated 38,500 vessels were affected by GNSS jamming in an eight-month window in 2025, alongside thousands of affected European flights.

The sustainable-development case. Inverting the usual framing, this report asks which UN SDGs would be set back by UK PNT loss rather than advanced by PNT. Eight goals, covering food security, health, energy, economic growth, infrastructure, sustainable cities, climate and marine life, carry a defensible, evidence-based dependency; a further four carry moderate, supporting linkages. This is a materially narrower and more defensible claim than asserting PNT supports all 17 goals and gives PNT investment cases a sustainable-development framing alongside the existing economic and national-security ones.

The enterprise case. Using financial services as an illustrative sector, chosen because its operational-resilience regulation is the most advanced in the UK, yet a direct review of the Financial Conduct Authority’s (FCA’s) Operational Resilience Policy Statement PS21/3 found no explicit mention of GNSS, GPS or PNT anywhere in its text. The report translates the national and SDG analysis into five board-level risks any business faces: supply chain disruption, financial transaction integrity failure, safety-critical/liability exposure, digital infrastructure/cyber-

¹ GNSS is a macro name for systems such as the United States’ Global Positioning System (GPS)

attribution disruption, and the governance failure that can convert any of the first four into a potentially uninsured, board-level liability and assurance crisis.

A recurring, commercially decisive finding is that standard commercial insurance is poorly matched to PNT/GNSS disruption: property and business-interruption cover requires physical damage that a signal-loss event typically doesn't cause, cyber cover is often silent on satellite-linked losses, and liability for jamming or spoofing turns on a difficult, fact-specific test of malicious intent. A business that has not deliberately closed this gap should assume it is substantially uninsured for a PNT disruption event. For organisations, the issue is not simply PNT dependency, but whether important services can remain within tolerance when underlying timing, communications and recovery infrastructure are tested under severe-but-plausible disruptions².

The conclusion and route to adoption. The national strategic, SDG and enterprise cases are not separate arguments but three expressions of the same underlying dependency. Technology options to mitigate PNT loss already exist and further capabilities are emerging; the residual strategic gap is implementation at scale, integration into operational processes, routine exercising and evidence that fallback arrangements hold under severe-but-plausible disruption.

The report therefore distinguishes **asserted** from **evidenced** resilience: ownership of backup technology or a contingency plan is insufficient unless an organisation can demonstrate dependency mapping, credible failure-mode analysis, independent alternatives and continuity within defined tolerances.

The policy task is to make that standard routine through existing mechanisms: board accountability, sector guidance and regulation, public procurement, exercising and assurance, incident reporting, insurance and supply-chain requirements.

The report recommends three immediate strands of work: strengthen the evidence available to future National Risk Register and departmental risk-assessment cycles through a reconciled UK economic-loss model, cross-sector dependency analysis and a common PNT assurance profile; test and implement resilience through (initially) financial-services and rotating sector exercises; and sustain delivery through a national implementation dashboard and a government–regulator–industry working groups. For organisations, the practical test is whether important services can remain within tolerance when timing, communications and recovery infrastructure are disrupted, degraded, denied, or deceived.

² Defined in [1] Financial Conduct Authority. "PS21/3 Building Operational Resilience." Financial Conduct Authority. <https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience> (accessed 2026).

Contents

Executive Summary.....	2
Contents.....	4
1 Purpose and Scope.....	6
1.1 In scope.....	6
1.2 Out of scope	6
1.3 How to use this document	6
1.4 Principles used in the document.....	7
2 Context and Case.....	8
2.1 What has already been established	8
2.2 From dependency to duty	8
2.3 Not every dependency is navigation	9
2.4 Why this matters now	9
3 Report Objectives	10
4 Analysis Baseline.....	11
4.1 The baseline data	11
4.2 Assessment dimensions	12
5 Strategic Risks	13
5.1 Mapping and posture	13
5.2 Priority tiered strategic risks.....	13
6 PNT Loss and the UN Sustainable Development Goals (SDGs).....	16
7 Risk to Business Continuity – Learning from the Enterprise Perspective	19
7.1 Why financial services as the illustrative sector	19
7.2 The enterprise risk register, in brief	20
7.3 Where the risk crystallises: insurance and liability.....	21
7.4 What this adds to the strategic and SDG analysis	21
8 Synthesis and analysis	23

8.1	From asserted to evidenced resilience	23
8.2	From awareness to adoption. Mechanisms for evidenced PNT resilience.....	24
8.3	Supporting recommendations	26
8.4	A Prepare/Absorb/Recover/Adapt checklist	26
Appendix A. PNT Risk Taxonomy and Source Category Reference.....		28
Appendix B. Full Longlist of Risks Considered.....		29
Appendix C – 8 Strategic Risks in detail		31
C1.	Risk 1 – Cascading Critical National Infrastructure Single Point of Failure	31
C2.	Risk 2 – Severe Macroeconomic Disruption from GNSS Outage.....	33
C3.	Risk 3 – Multi-Modal Transport Safety and Operability Failure	35
C4.	Risk 4 – Telecoms, digital infrastructure and trusted-time failure	37
C5.	Risk 5 – Emergency Services and Public Safety Degradation.....	39
C6.	Risk 6 – Energy System Stability and Control Degradation	41
C7.	Risk 7 – Adversarial PNT Denial and Hybrid/State Threat Escalation	43
C8.	Risk 8 – Space-Weather Multi-Hazard Catastrophe	45
Appendix D. Business Risk Register and Insurance/Liability Detail.....		47
D1	Methodology and frameworks applied	47
D2	The five strategic risks to a generic business – full register	48
D3	Insurance Aspects: Liabilities and Risks from Insufficient PNT Resilience Planning	55
D4	Applying the frameworks: a practical approach	59
Appendix E: References		60
Appendix F: Document administration.....		65

1 Purpose and Scope

This report provides an assessment of the top strategic risks arising from loss, degradation or corruption of Position, Navigation and Timing (PNT) services to the United Kingdom, and extends that assessment across two further lenses: the United Nations Sustainable Development Goals (SDGs), and the equivalent strategic risk picture facing an individual commercial business.

1.1 In scope

- The eight priority strategic risks to the UK from loss, jamming, spoofing or systemic failure of GNSS-derived PNT, ranked and summarised in Section 5, with full supporting detail in the Appendices.
- A dedicated cross-reference of PNT loss against all 17 UN Sustainable Development Goals (SDGs), summarised in Section 6. A full analysis can be made available.
- A translation, Section 7, of the national strategic risk and SDG analysis into an enterprise-facing strategic risk register, illustrated using a financial-services exemplar, with the analysis in Appendices.

1.2 Out of scope

- This is not a national risk assessment and does not substitute for the Cabinet Office National Risk Register or any sponsor department's own risk register. It is an open-source, multi-source synthesis intended to inform, not replace, those processes.
- It does not provide a probabilistic loss-exceedance model. Quantitative figures are reproduced from named primary sources with their original scenario assumptions preserved, not re-derived.
- It does not offer legal, insurance or investment advice. The business chapter and Appendix D insurance analysis are a research synthesis for awareness, not a substitute for professional advice on a specific organisation's programme.
- It does not attempt a full technical options appraisal of specific resilient-PNT technologies (eLoran, UK SBAS, quantum sensing), these are referenced only where they bear directly on risk mitigation.

1.3 How to use this document

Sections 1–7 form the core narrative and are written for a senior-level reader: each strategic risk is given a brief overview only, sufficient to support prioritisation and decision-making without requiring the reader to absorb full technical or economic detail in-line. Full risk-by-risk detail –

mechanism, cross-source corroboration, quantitative indicators and dedicated references is placed in Appendices.

Section 8 provides a synthesis of this analysis with a recommended programme of work to address the core findings.

1.4 Principles used in the document

- Multi-source corroboration – findings are retained only where at least two independent source categories (UK government, US government, Australian government, international/allied, academic, World Economic Forum (WEF), insurance) describe the same failure mode or consequence class.
- Primary sources only – quantitative estimates are reported exactly as published by named sources, with original scenario assumptions and ranges preserved rather than blended or re-derived.
- Resilience-domain framing – risk is analysed through the physical, information, cognitive and social domains and the plan/prepare → absorb/resist → respond/recover → adapt resilience curve, following the resilience-engineering framework [2].
- Honest strength grading – where a linkage (for example, to a specific SDG) is weak or indirect, this report says so rather than inflating it. Overclaiming weak links weakens the credibility of the genuinely strong ones.

2 Context and Case

2.1 What has already been established

UK government analysis already treats GNSS as an “invisible utility” underpinning banking, transport and “almost all the UK’s critical national infrastructure” [3], while explicitly warning that national awareness of that dependence is “out of step with our actual dependence upon it” [4]. The 2025 National Risk Register already registers severe space weather, GNSS constellation failure, disruption of space-based services and states threats to PNT as standing national security risks [3], and the Government’s framework for greater PNT resilience – the National PNT Office, National Timing Centre, eLoran proposal, holdover clocks and a cross-government PNT Crisis Plan – is the principal existing policy response [5].

This assessment does not seek to duplicate that machinery. It exists to (a) cross-reference UK evidence against US, Australian, international, academic, WEF, and sector sources so that stakeholders and recipients see a corroborated, not merely UK-sourced, picture; (b) make the case explicit in SDG terms, which existing UK PNT policy documents do not currently do; and (c) carry the national analysis down to the level an individual regulated business can act on, which is likewise absent from current government guidance – notably, a direct review of the Financial Conduct Authority’s (FCA) own Operational Resilience Policy Statement PS21/3 found no explicit mention of GNSS, PNT or GPS anywhere in its published text [1], a regulatory blind spot this report treats as itself part of the strategic risk picture.

2.2 From dependency to duty

The central policy challenge is not simply whether the United Kingdom recognises PNT risk. It is whether organisations that depend on trusted position, navigation or timing are compelled to understand that dependency, mitigate it proportionately and demonstrate that their mitigations work. Awareness alone does not create resilience.

This paper therefore moves beyond the case for backup PNT. It argues for a transition from asserted resilience to evidenced resilience. Organisations should be able to identify their material PNT dependencies, understand credible failure modes, maintain proportionate alternatives and demonstrate through testing and exercising that essential functions can continue through disruption or deception. Section 8 sets out what evidenced resilience means in practice and the mechanisms that could drive adoption.

PNT should be regarded as enabling national infrastructure. Its importance does not depend on national ownership of a satellite constellation or signal source; electricity, telecommunications and water are treated as infrastructure because society depends upon their reliable delivery. Trusted time and position increasingly merit the same treatment.

2.3 Not every dependency is navigation

“GPS dependency” is an inadequate shorthand for the policy problem. Position, navigation and timing are related but distinct dependencies, with different users, failure modes and consequences.

Position and navigation failures may affect transport, logistics, emergency response, autonomy and defence manoeuvre. Timing failures may be less visible, but can be acute for telecommunications, financial-market infrastructure, data centres, electricity networks, distributed systems and synchronised operational technology.

Organisations should therefore assess PNT as three linked dependency classes – Position, Navigation and Timing – rather than treating it as a single navigation issue. A board may have no material vehicle-navigation exposure while retaining a significant dependence on externally derived time.

This distinction has direct implications for risk ownership and resilience assurance. The relevant question is not whether an organisation “uses GPS”, but whether any essential service depends on trusted location, navigation or synchronised time; which dependency is material; how it can fail; and whether the service remains within tolerance when that dependency is degraded, denied or corrupted.

2.4 Why this matters now

Real-world interference affecting GNSS-derived PNT has moved from a theoretical vulnerability to an observed operational pattern. GPS jamming affected an estimated 38,500 vessels between April and November 2025, concentrated in the Black Sea, Baltic and Persian Gulf [6], and over 2,300 Ryanair flights, plus dozens of British Airways and easyJet flights, were affected by suspected jamming over the Baltic in a single reporting period [7]. Insurers and reinsurers are repricing this reality: Lloyd’s published a dedicated systemic risk scenario on extreme space weather in March 2025 modelling a probability-weighted USD 2.4 trillion global economic loss over five years [8], and the ‘CRO Forum’ – representing the Chief Risk Officers of major European (re)insurers – now names GNSS/GPS jamming and spoofing, the 2022 Viasat KA-SAT cyberattack, and space weather among the material, growing exposures for the sector [9].

Against this backdrop, there is a narrow window in which evidence-led analysis can shape both national policy investment and enterprise-level resilience practice before, rather than after, a significant disruption event.

Operational resilience doctrine turns on the ability to remain within tolerance under severe-but-plausible disruption. In that context, the practical question is not whether a PNT-loss scenario can be described as plausible, but whether the underlying timing, communications and recovery

infrastructure can sustain critical services when that scenario occurs. Where resilient PNT is absent or untested, severe-but-plausible can become a paper assumption rather than an evidenced capability.

3 Report Objectives

This report has four objectives:

1. Rank the strategic risks arising from PNT loss with sufficient rigour and sourcing that recipients can use the ranking to prioritise policy and investment attention.
2. Establish an explicit and honestly graded linkage between PNT resilience and the 17 UN Sustainable Development Goals (SDG), so that PNT investment cases can be framed in sustainable-development as well as national-security and economic terms.
3. Translate the strategic risk and SDG analysis into a strategic risk register that an individual commercial board can act on, including the specific insurance and liability exposure that follows from inadequate planning – illustrated through a representative sector exemplar.
4. Package the above so that stakeholders, and any regulator, department or company, receive a document that is briefing-ready at the summary level and audit-ready at the appendix level.

4 Analysis Baseline

4.1 The baseline data

Seven source categories (Table 1) were reviewed to build the evidence baseline for the risk analysis, each retained in the corroboration tables in the Appendices.

Table 1: Sources used in baseline data acquisition

Source category	Representative sources used
UK government and UK-linked analysis	Blackett Review; GOV.UK PNT Overview; National Risk Register 2025/2023; London Economics/Innovate UK economic impact study; UK Space Alliance resilient-PNT economics; NPL/National Timing Centre programme materials; HCWS1073
US government	DHS National Risk Estimate on GPS disruptions; CISA GPS interference insights and PNT vulnerability fact sheets; DHS S&T resilient-PNT best practices; Executive Order 13905; RTI International economic benefits of GPS study
Australian government / research ecosystem	FrontierSI Resilient PNT report and white paper; Australian Academy of Science space-based PNT working group report; CISC PNT factsheet
International / allied	EUSPA/Galileo resilience and authentication materials; NATO STO PNT/NAVWAR technical notes [57][58][59]
Academic / institutional	Peer-reviewed and preprint literature on GNSS jamming/spoofing, interference detection and infrastructure interdependency
World Economic Forum	Global Risks Report 2025/2026 taxonomy and rankings
Insurance / catastrophe risk	Lloyd's extreme space weather systemic scenario; Cambridge Centre for Risk Studies HELIOS solar-storm scenario; Swiss Re satellite constellation risk analysis; CRO Forum space-risk report

The business-chapter baseline additionally draws on ISO 22301, BS 65000, COSO ERM 2017, ISO 31000:2018, the UK Corporate Governance Code 2018, Companies Act 2006 s.172, FCA PS21/3 and PRA SS1/21, and current insurance-market and legal-liability commentary [10-16]; the SDG baseline draws principally on the joint UNOOSA–European GNSS Agency study ST/SPACE/71 [17].

Risks were retained only where at least two independent source categories described the same failure mode or consequence class, and were then weighted by breadth of multi-source corroboration and UK policy salience, not by a single quantitative loss figure, since the available

economic estimates use materially different scenario assumptions (24-hour, 5-day, 7-day and 30-day outage windows; pure GNSS-only outage versus multi-hazard space-weather events) that are not directly comparable. Section 5 sets out the resulting assessment dimensions and priority tiers.

4.2 Assessment dimensions

Each candidate risk was assessed against four dimensions: breadth of cross-source corroboration (how many independent source categories describe the same failure mode); UK policy salience (whether the risk is already registered in UK government instruments such as the National Risk Register); potential severity and cascade reach (whether the consequence stays within one sector or propagates across CNI); and time-to-manifestation (whether the risk is already observed in the field or remains a plausible but not-yet-realised scenario).

5 Strategic Risks

5.1 Mapping and posture

In this report, the risk of PNT loss was additionally mapped against the WEF's 2023 & 2025 global risk taxonomy. PNT loss is not a standalone WEF category but triggers or amplifies several top-ranked ones: disruptions to critical infrastructure (a definition that explicitly includes satellites), cyber espionage and warfare, state-based armed conflict, geoeconomic confrontation, and non-weather-related natural disasters (which explicitly includes geomagnetic storms) [18].

The UK's current resilience posture already addresses several of these risks in principle through the National PNT Office, National Timing Centre, eLoran proposal and PNT Crisis Plan [19].

The cross-source evidence base indicates that the residual strategic gap is not primarily technological availability, but implementation at scale, routine exercising, and evidence that fallback arrangements will hold under severe-but-plausible disruption. This matters because resilience is only demonstrated where alternative PNT arrangements are deployed in operations, understood by operators, and exercised often enough to expose hidden dependency and recovery weaknesses.

In resilience terms, capability that has not been implemented, mapped to dependencies, and tested in severe-but-plausible scenarios should not be assumed to exist when needed.

5.2 Priority tiered strategic risks

This section defines a strategic risk as any high-level threat, event, or systemic vulnerability that can severely damage a country's vital national interests, safety, economy, or long-term governing objectives.

Eight risks are grouped into three priority tiers reflecting corroboration breadth and cascade reach: Tier 1 (Risks 1–3) are cross-cutting, high-corroboration risks with the broadest CNI reach; Tier 2 (Risks 4–6) are significant sector-specific risks with strong corroboration but narrower immediate reach; Tier 3 (Risks 7–8) are lower-frequency but potentially catastrophic tail risks with a distinct national-security or natural-hazard character.

They are ranked below, Table 2, by breadth of multi-source corroboration and UK policy salience.

Table 2: Ranked strategic risks

Rank	Strategic risk	One-line description
1	Cascading CNI single point of failure	GNSS as a “system of systems” failure mode that cascades across interdependent UK critical infrastructure.

Rank	Strategic risk	One-line description
2	Severe macroeconomic disruption	Multi-billion-pound-per-day-scale economic shock from short GNSS outages, with compounding logistics and productivity losses.
3	Multi-modal transport safety and operability failure	Simultaneous degradation of road, maritime, aviation and rail navigation, traffic management and port logistics.
4	Telecoms, digital infrastructure and trusted-time failure	Telecoms, digital infrastructure and trusted-time failure: loss or corruption of precise timing that underpins mobile, fixed, broadcast and data-centre networks, and increasingly IT services, virtualised platforms, security logging and digital trust services, cascading into other CNI.
5	Emergency services and public safety degradation	Degraded location, dispatch, communications and justice-system capability at the point of greatest societal need.
6	Energy system stability and control degradation	Timing-dependent grid monitoring/control degraded, with dual exposure via space weather.
7	Adversarial PNT denial and hybrid/state threat escalation	Intentional jamming, spoofing and electronic attack as a low-cost, high-leverage tool against UK CNI and defence support.
8	Space-weather multi-hazard catastrophe	Severe solar/geomagnetic events that simultaneously degrade GNSS, power and satellite services at national/global scale.

Brief overviews of each risk follow. Full mechanism detail, cross-source corroboration tables, quantitative indicators and dedicated references for each risk are in Appendix C.

5.2.1 Risk 1 (Tier 1) – Cascading CNI single point of failure

GNSS has become a cross-cutting dependency inside a UK “system of systems”, such that loss or corruption of PNT does not stay inside one sector but propagates through communications, energy, transport, emergency services, finance and government functions [3, 4]. This is the underlying rationale for the National PNT Office, the cross-government PNT Crisis Plan and the National Timing Centre [20].

5.2.2 Risk 2 (Tier 1) – Severe macroeconomic disruption

A sustained UK GNSS outage would impose a rapid, billions-of-pounds-scale economic shock: GOV.UK’s 2023 update puts UK GNSS benefits at £13.62bn per annum, a 24-hour loss at £1.42bn and a 7-day loss at £7.64bn [21], while the earlier London Economics five-day-outage study

found £5.2bn of impact, 88% of it concentrated in road, maritime and emergency/justice services [22].

5.2.3 Risk 3 (Tier 1) – Multi-modal transport safety and operability failure

Road, maritime, aviation and increasingly rail navigation can degrade simultaneously in a PNT outage, creating safety risk, congestion and supply-chain delay; London Economics attributes 37% of five-day UK outage impacts to road and 21% to maritime applications [22].

5.2.4 Risk 4 (Tier 2) – Telecoms, digital infrastructure and trusted-time failure

UK telecoms and digital infrastructure use GNSS as a primary source of precise time and frequency synchronisation. That dependency now extends beyond network transport into data centres, virtualised compute environments, identity and access services, event logging, distributed transaction ordering and digital signing or trusted-timestamp functions that rely on coherent system time.

5.2.5 Risk 5 (Tier 2) – Emergency services and public safety degradation

Emergency and justice services are among the highest-utility GNSS users in the UK. London Economics finds loss of GNSS would impose about £1.5bn of impact on emergency and justice services over five days, roughly 30% of total estimated outage costs [22].

5.2.6 Risk 6 (Tier 2) – Energy system stability and control degradation

Timing-dependent wide-area monitoring and control – phasor measurement units in particular – create rising strategic exposure, compounded by the fact that the same space-weather events that deny GNSS also stress high-voltage grids [3].

5.2.7 Risk 7 (Tier 3) – Adversarial PNT denial and hybrid/state threat escalation

Intentional jamming and spoofing convert PNT dependence into a national-security problem: DHS scenario analysis describes spoofing that can induce timing errors of hundreds of microseconds and position errors of tens of metres while receivers remain “confident” – more dangerous than an obvious outage [23].

5.2.8 Risk 8 (Tier 3) – Space-weather multi-hazard catastrophe

Severe space weather is the clearest nationally registered, physically plausible pathway to simultaneous PNT, power and satellite loss. Lloyd’s systemic scenario models a probability-

weighted USD 2.4 trillion global economic loss over five years, with a modelled ~USD 697bn hit to Europe [8].

6 PNT Loss and the UN Sustainable Development Goals (SDGs)

The 2030 Agenda for Sustainable Development commits UN member states, including the UK, to 17 Goals and 169 targets [24, 25]. Assessing with respect to these SDGs helps organisations find hidden financial threats, spot new market opportunities, and contextualise within societal needs.

Space-based capabilities, and PNT specifically, are recognised by the UN Office for Outer Space Affairs (UNOOSA) and the European GNSS Agency as material enablers of SDG delivery. Their joint study *Space for the Sustainable Development Goals* documents concrete linkages across the full Goal set, and UNOOSA’s dedicated Space4SDGs programme, together with the International Committee on GNSS (ICG), exists specifically to coordinate this contribution [17, 26, 27]. The European Space Agency similarly frames its own programme explicitly in SDG terms [28].

This section inverts that framing for risk purposes: rather than asking how PNT *advances* the SDGs, it asks which Goals would be set back, and by how much, if UK PNT services were degraded, denied or corrupted. Table 3 summarises the linkage strength for all 17 Goals, graded honestly – strong, moderate or weak/indirect – rather than uniformly asserting a strong link. Full Goal-by-Goal analysis, including the specific mechanism and evidence for each rating, is provided in [29].

Table 3: PNT loss impact by SDG (summary)

SDG	Linkage strength	Rationale (summary)
SDG 1 – No Poverty	Weak / indirect	PNT-enabled precision agriculture and financial inclusion support poverty reduction, but the causal chain is long.
SDG 2 – Zero Hunger	Strong	GNSS is a core enabler of precision agriculture (guidance, mapping, variable-rate application); UK food and agriculture GNSS benefit was estimated at ~£285m/year, with a five-day outage costing £134–156m.
SDG 3 – Good Health and Well-being	Strong	PNT underpins emergency medical response, ambulance navigation and telemedicine geolocation; UK emergency and justice services’ GNSS benefit was estimated at ~£2.1bn/year, with a five-day loss on the order of £1.5bn.

SDG	Linkage strength	Rationale (summary)
SDG 4 – Quality Education	Weak / indirect	Only marginal, indirect linkage (e.g. connectivity-dependent remote learning).
SDG 5 – Gender Equality	Weak / indirect	No direct mechanism identified; any linkage is via general economic/connectivity effects.
SDG 6 – Clean Water and Sanitation	Moderate	Water utility monitoring and network operations increasingly use GNSS timing for SCADA synchronisation.
SDG 7 – Affordable and Clean Energy	Strong	Grid wide-area monitoring, protection and control (phasor measurement units) depend on GNSS-derived timing; the same space-weather hazard threatens both PNT and grid stability directly.
SDG 8 – Decent Work and Economic Growth	Strong	GOV.UK values UK GNSS economic benefit at £13.62bn/year with billions-per-day-scale exposure to outage; this is one of the most directly quantified linkages in the analysis.
SDG 9 – Industry, Innovation and Infrastructure	Strong	PNT is foundational, cross-cutting infrastructure for transport, telecoms, energy and construction; it is explicitly named as CNI-relevant in UK, US and EU sources.
SDG 10 – Reduced Inequalities	Weak / indirect	No direct evidence-based mechanism identified beyond general economic effects.
SDG 11 – Sustainable Cities and Communities	Strong	Urban traffic management, public transport, utilities and emergency response in cities are materially PNT-dependent; London Economics attributes ~30% of five-day outage cost to emergency/justice services alone.
SDG 12 – Responsible Consumption and Production	Moderate	Precision logistics and route optimisation reduce fuel/emissions waste; GNSS timing underpins supply-chain traceability systems.
SDG 13 – Climate Action	Strong	PNT is part of the wider space-enabled infrastructure used for climate monitoring, environmental observation, resilient energy operation and climate-related hazard response; loss of resilient timing also weakens digital, and energy systems needed to withstand and recover from climate-linked disruption.

SDG	Linkage strength	Rationale (summary)
SDG 14 – Life Below Water	Strong	Maritime navigation, marine traffic management, fisheries monitoring, offshore operations and port logistics are directly GNSS-dependent; disruption increases collision, grounding and marine pollution risks while degrading safe and efficient use of the marine environment
SDG 15 – Life on Land	Moderate	Precision agriculture, land-use monitoring and conservation tracking use GNSS positioning.
SDG 16 – Peace, Justice and Strong Institutions	Weak / indirect	Justice-system logistics and law-enforcement dispatch are PNT-touched, but the SDG’s core institutional-strength mechanisms are largely PNT-independent.
SDG 17 – Partnerships for the Goals	Moderate	International PNT interoperability (GPS/Galileo/GLONASS/BeiDou) and UN/UNOOSA coordination bodies such as the International Committee on GNSS exemplify multilateral partnership in service of the Goals.

Eight Goals – SDG 2, 3, 7, 8, 9, 11, 13 and 14 – carry a defensible, evidence-based dependency on resilient PNT, with SDG 6, 12, 15 and 17 as supporting moderate linkages. This is a materially narrower claim than “PNT supports all 17 SDGs” and is deliberately so. The credibility of the strong linkages (food security, health, energy, economic growth, infrastructure, sustainable cities, climate and life below water) depends on this report not inflating the weaker ones.

The clearest cross-cutting implication is that PNT resilience investment cases can now legitimately cite sustainable-development impact, in addition to economic and national-security framings, when engaging with departments, regulators or investors for whom SDG alignment is a formal appraisal criterion.

7 Risk to Business Continuity – Learning from the Enterprise Perspective

This enterprise lens matters because PNT dependence is where strategic risk meets the operational-resilience test. For regulated firms, severe-but-plausible scenario testing is intended to show that important business services can remain within impact tolerances under disruption.

If a firm has not identified where timing underpins those services and has not tested whether underlying infrastructure can continue to deliver without trusted PNT, then the scenario has not been fully mapped, the resilience claim is weak, and the associated insurance exposure may remain unrecognised.

Sections 4–6 established the strategic-level risk and sustainable-development picture. This chapter translates that picture into the terms a commercial board, audit committee or chief risk officer must act on: business continuity, resilience-domain exposure, and because it is where the strategic risk ultimately crystallises financially – insurance and director liability. Full detail, including the complete risk register, resilience-domain mapping and the six-part insurance/liability analysis, are in Appendices C and D.

7.1 Why financial services as the illustrative sector

Financial services is used here for three reasons. First, it is the sector where the UK regulatory picture is most advanced and yet most explicitly silent on PNT: a direct review of the FCA’s Operational Resilience Policy Statement PS21/3 – the primary instrument requiring UK regulated firms to identify important business services, set impact tolerances and test severe-but-plausible scenarios – found no explicit reference to GNSS, GPS or PNT anywhere in its text [4], a gap mirrored in the PRA’s parallel supervisory statement SS1/21 [12] and in the FCA’s 2022 discussion paper on critical third parties [23].

Second, financial services carry some of the most acute PNT-timing dependencies of any sector: high-frequency and algorithmic trading, MiFID II-mandated transaction timestamping, interbank settlement, and ATM/card network synchronisation all rely on GNSS-derived precise time. The London Economics five-day-outage study’s finding that financial services was among the impacted sectors is not incidental [21].

Third, the sector is a useful stress-test for the whole enterprise risk register because it combines every category in Appendix D at once – supply chain, financial transaction integrity, safety-critical/liability, digital infrastructure/cyber-attribution and governance/insurance – in a single regulated entity, making it the clearest single lens for the synthesis below. The conclusions nonetheless generalise: any organisation with safety-critical operations, time-stamped transactions, distributed logistics or externally-audited resilience obligations faces a structurally

similar exposure and retains the generic risk register alongside the financial-services framing so the analysis remains directly usable outside that sector.

7.2 The enterprise risk register, in brief

This paper reframes the strategic-level risk picture for an individual, generic business. It applies three complementary lenses:

1. Resilience engineering – which models resilience as a function of time (Plan/Prepare → Absorb → Recover → Adapt) and space (Physical, Information, Cognitive and Social domains), and explicitly distinguishes resilience thinking from conventional threat-by-threat risk management [2].
2. UK business continuity and corporate governance practice – ISO 22301, BS 65000, Cabinet Office Business Continuity Management guidance, the UK Corporate Governance Code 2018, and section 172 of the Companies Act 2006 [10, 14-16, 30].
3. Strategic company risk register conventions – COSO ERM 2017 and ISO 31000:2018, expressed through the likelihood/impact/control/residual-risk structure used in UK corporate risk registers and annual report risk disclosures [13, 14].

Applying these lenses identifies five board-level risks, Table 4, that a generic UK business faces from loss of PNT services:

Table 4: Board level enterprise risks for business

Risk	Strategic/SDG root cause	Enterprise manifestation
Supply chain and logistics disruption	Risks 1–3 (cascading CNI, macroeconomic shock, multi-modal transport); SDG 8, 9, 11, 12	Fleet, freight and port-logistics visibility loss; contingent business interruption exposure even where the firm's own sites are undamaged.
Financial transaction integrity failure	Risks 1, 4 (cascading CNI, telecoms/timing); SDG 8, 9	MiFID II timestamp integrity, settlement synchronisation and high-frequency trading risk from timing-source corruption, not just outage.
Safety-critical operations and liability	Risks 3, 5, 7 (transport safety, emergency services, adversarial denial); SDG 3, 11, 16	Autonomous/assisted vehicle, drone, surveying and asset-tracking liability exposure where PNT integrity is silently assumed.

Risk	Strategic/SDG root cause	Enterprise manifestation
Digital infrastructure and cyber-attribution	Risks 4, 6, 7 (timing sync, energy control, adversarial denial); SDG 7, 9	Data-centre and network timing degradation; spoofing incidents that are hard to distinguish from cyberattack, complicating incident response and insurance claims.
Governance failure and insurance/liability gap	Cross-cutting (Risks 1–8); all strong-linkage SDGs	The board has not identified PNT/GNSS dependency as a principal or emerging risk, failure to test a foreseeable, already-registered national risk, crystallising as D&O, PI and coverage-gap exposure – the subject of §7.3 below. Can be considered a meta-risk.

7.3 Where the risk crystallises: insurance and liability

The enterprise risk only becomes a board-level problem when it converts into financial or legal exposure, and Appendix D sets out six specific mechanisms by which that happens:

- a coverage gap for PNT disruption, since standard business-interruption insurance only pays out for physical damage, and a GNSS outage causes no physical damage [31–35].
- cyber-policy ambiguity over whether jamming/spoofing is a “cyber” peril at all, sharpened by London Market Association war-exclusion clauses [36].
- director and officer liability where a foreseeable, already-registered national risk was not tested [37, 38], with derivative-claim mechanics under UK company law providing the route by which shareholders could pursue that failure [39].
- professional indemnity and product liability exposure for surveying, autonomous-systems and sensor-dependent providers [40–42].
- contractual/SLA liability cascading through supply chains [43]; and
- a hardening insurer/underwriter view of PNT and space-weather risk as an emerging systemic exposure requiring dedicated scenario modelling [44, 45].

7.4 What this adds to the strategic and SDG analysis

Read together, Sections 5–7 support one central conclusion: the strategic risk case, the SDG case and the enterprise case are not three separate arguments but three facets of the same underlying dependency, and they reinforce rather than compete with one another.

A recurring and commercially decisive finding is that standard commercial insurance is poorly matched to PNT/GNSS disruption. Property and business interruption cover is triggered by physical damage, which a signal-loss event typically does not cause; cyber cover is often silent or excluded for satellite infrastructure; and liability for jamming/spoofing turns on a difficult, fact-specific test of malicious intent and state attribution.

A business that has not deliberately addressed this gap should assume it is substantially uninsured for a PNT disruption event, regardless of the extent of its general insurance programme.

A risk owner/sponsor can use Section 5 to justify infrastructure investment, Section 6 to justify it in sustainable-development terms to different stakeholders, and Section 7 to make the case directly to regulated firms in language (board liability, insurance coverage, audit findings) that a corporate audit committee, rather than a government analyst, will act on.

Fresnillo plc's published integrated-reporting risk heat map, an unrelated FTSE 250 example used here purely as illustrative, shows how a board-level risk register visualises likelihood against impact in exactly the format a sponsor could ask a regulated firm to complete for PNT dependency [46]. Appendix D sets out that exercise for the financial-services exemplar in full.

For a board, the practical test is whether PNT resilience is evidenced through dependency mapping, tolerances, exercising and assurance, not merely asserted through policy or asset ownership.

8 Synthesis and analysis

Seven cross-risk patterns emerge from reading the strategic, SDG and enterprise analysis together:

1. PNT is part of the enabling infrastructure that determines whether severe-but-plausible testing is credible at all. This matters commercially because a firm that has not evidenced its dependency may face both a resilience failure and a coverage gap. The service can fail even where no physical damage has occurred, while insurance response remains uncertain or absent.
2. Timing, not just positioning, is the more fragile and more consequential dependency – telecoms, energy, and financial-transaction integrity depend on precise time far more than on position, yet public and boardroom attention still concentrates on “GPS for navigation”. Organisational resilience claims are only as strong as the timing, synchronisation and recovery assumptions on which they rest.
3. Multi-hazard convergence is under-appreciated – severe space weather is simultaneously a PNT threat, an energy-grid threat and a satellite-services threat, so treating it in a single-hazard silo understates its real consequence.
4. Adversarial denial and natural/technical failure produce near-identical symptoms at the receiver, which complicates both incident response and insurance-claim attribution – a theme that runs from Risk 7 in Section 5 through to the cyber-policy ambiguity discussed in Section 7 and Appendix D.
5. The SDG linkages that matter most (7, 8, 9, 11, 13, 14) are the same clusters that dominate the national risk register – energy, economy, infrastructure, cities, climate-adjacent hazards and maritime – which is itself evidence that the mapping in Section 6 is grounded.
6. Regulatory silence on PNT (Section 7.1) is a finding in its own right, not just a gap to note – it means the enterprise exposure in Appendix D currently sits largely untested even in the most operationally-resilience-mature UK sector.
7. Technology options to mitigate PNT loss already exist (with a development pipeline strong). The strategic failure mode is non-adoption, weak integration into business and operational processes, and insufficient exercising against realistic scenarios.

8.1 From asserted to evidenced resilience

There is a distinction between asserted and evidenced resilience. Ownership of an alternative receiver, holdover clock, terrestrial timing feed, inertial system or contingency plan does not

itself demonstrate resilience. The relevant evidence is that an organisation has mapped its material PNT dependencies; analysed credible loss, degradation and deception scenarios; deployed sufficiently independent alternatives; and tested whether important services remain within defined tolerances through disruption and recovery. This matters because PNT failure may be silent, partial or misleading: a spoofed timing or position source can appear available while corrupting downstream decisions, records and controls. The assurance question is therefore not “what backup is installed?” but “what evidence shows that the service, its operators and its recovery arrangements will perform under severe-but-plausible PNT disruption?”. The policy objective is to make PNT resilience an evidenced operational outcome, proportionate to the consequence of failure.

8.2 From awareness to adoption. Mechanisms for evidenced PNT resilience

The principal residual gap is not a simple absence of technical options; it is non-adoption, weak operational integration and insufficient exercising. The policy question is therefore how recognised PNT dependency becomes action. Existing resilience, cyber, sectoral and procurement mechanisms should be used proportionately to make the standard of evidenced resilience set out above routine across essential services, rather than creating a wholly separate PNT regulatory regime.

Table 5: Mechanisms for evidenced PNT resilience

Adoption mechanism	What it changes	Practical PNT application
Board accountability	Makes dependency visible to those responsible for risk appetite, investment and residual risk.	Require material PNT dependency maps, named ownership, failure-mode analysis, impact tolerances and board review for safety- or mission-critical services.
Sector standards and regulation	Turns recognised risk into minimum, proportionate resilience expectations.	Include PNT in future sector guidance, resilience profiles, codes of practice and secondary requirements where timing, position or navigation supports an essential function.
Public procurement	Makes resilience a condition of contract and market access.	Central government and CNI authorities require suppliers to demonstrate proportionate PNT resilience, with requirements flowing to critical subcontractors.

Adoption mechanism	What it changes	Practical PNT application
Exercising and assurance	Distinguishes purchased fallback from proven continuity	Require realistic GNSS-denied, spoofing and timing-degradation exercises; test detection, escalation, fallback, recovery, evidential logging, and demonstrate that the services remain within tolerance.
Incident reporting and situational awareness	Creates a shared national picture of material disruption and manipulation.	Define common thresholds and taxonomies for significant PNT interference, spoofing, timing degradation and loss-of-confidence events, while retaining sector ownership.
Insurance and finance	Prices unevidenced dependency and rewards tested resilience.	Encourage dependency assessments, tested alternatives and exercising to inform coverage, terms, excesses, and underwriting appetite.
Customer and supply-chain requirements	Extends resilience expectations beyond the directly regulated entity.	Essential-service operators require critical suppliers to disclose relevant PNT dependence, continuity arrangements, assurance evidence, and incident-notification procedures.

- Cyber and essential services: PNT dependency becomes explicit in resilience assessments, sector guidance and future secondary requirements where it affects essential or digital services.
- National readiness: Consider PNT as a crisis- and conflict-readiness dependency across logistics, communications, energy, data and command, without presuming the content of proposed legislation.
- Insurance and finance: Encourage evidence of dependency mapping, alternative capability and exercising in underwriting conversations, while recognising that product development and risk pricing are market-dependent.

The case for greater PNT resilience is no longer solely a case for alternative technologies. It is a case for national adoption, embedding responsibility for trusted position, navigation and timing within the governance of essential services, defence readiness, supply chains, operational and organisational resilience.

The future architecture will be layered, combining satellite, terrestrial, networked, onboard and passive capabilities, with emerging technologies adopted where they provide meaningful independence or assurance. The assumption that a single source can remain trusted, available and sufficient under all conditions must end.

8.3 Supporting recommendations

The adoption mechanisms above identify how PNT resilience can be embedded in governance, regulation, procurement, and market practice. The following programme of work would strengthen the evidence base, test the approach and support implementation:

1. **Strengthen the national evidence base and risk-register interface.** Develop a reconciled UK-specific PNT-loss economic model, bringing together the differing 24-hour, five-day, seven-day and annual assumptions in existing studies into a transparent, sponsor-agreed scenario and loss framework. Use the resulting evidence, alongside this report's cross-sector risk taxonomy and SDG mapping, to inform future National Risk Register and relevant departmental risk-assessment cycles, without seeking to duplicate or substitute for them. In parallel, develop a cross-sector PNT dependency and assurance profile, drawing on the NIST PNT Profile model[47], to provide regulators, boards and essential-service operators with a consistent approach to dependency mapping, control selection and resilience evidence.
2. **Test and implement by sector.** Run an initial financial-services tabletop against a real firm's operational-resilience impact tolerances, followed by agreed remediation and re-testing. Establish a rotating programme of sector deep-dives, transport, energy, telecommunications and emergency services, each producing a sector-specific evidence and action annex in the style of Appendix D.
3. **Create durable delivery mechanisms.** Maintain a living dashboard against the Section 5 risk ranking to track delivery of the National Timing Centre, eLoran and PNT Crisis Plan. Convene a government-regulator-industry working group, initially covering financial services, telecommunications, energy and data infrastructure, to develop proportionate expectations for PNT resilience, incident-reporting triggers and an insurer-facing evidence framework.

8.4 A Prepare/Absorb/Recover/Adapt checklist

Using the "stages of resilience" [2], and consistent with the Royal Institute of Navigation's Prepare → Act → Recover best-practice model for PNT resilience [48]:

1. Plan/Prepare – Businesses need to conduct or commission a PNT-specific Business Impact Analysis; add PNT/GNSS dependency evidence to the enterprise risk register with

an explicit risk appetite statement; review the full insurance programme against the six liability areas noted in this report; ensure boards are informed sufficiently so that Corporate Governance Code and s.172 obligations are demonstrably discharged.

2. Act (Absorb) – Build “graceful degradation” (and evidence of it) into PNT-dependent processes (manual fallback procedures, holdover-capable clocks, independent position verification for safety-critical tasks); pre-agree an internal protocol for triaging an ambiguous-cause GNSS disruption so insurance notification(s) and technical responses are not delayed by classification uncertainty.
3. Recover – Define and test recovery time objectives (resilience requirements) for each PNT-dependent process; pre-identify which secondary processes and functions (including insurance policies) would be impacted for which failure mode and pre-position technical responses as well as ensuring that system response evidence (logs, timestamps, third-party attribution data) is available for subsequent analysis.
4. Adapt – Feed lessons from any near-miss or actual disruption back into the risk register, insurance renewal strategy and business continuity management plans; monitor the evolving external environment (national PNT resilience programmes, insurer product development, regulatory guidance) and update the business’s posture accordingly, consistent with ISO 22301 Clause 10 (evidence-led improvement).

Appendix A. PNT Risk Taxonomy and Source Category Reference

Candidate risks in this report are classified by primary failure mode and consequence class, producing eight non-overlapping categories:

Table 6: Risk taxonomy

Category	Definition	Example national risk (Section 5)
Cascading infrastructure failure	Loss propagates across interdependent CNI sectors rather than staying within one.	Risk 1
Macroeconomic shock	Direct GDP/output loss from outage, independent of any single sector mechanism.	Risk 2
Transport safety/operability	Degraded navigation, traffic management or logistics across one or more transport modes.	Risk 3
Telecoms/digital synchronisation	Loss of precise time/frequency reference underpinning networks and data infrastructure.	Risk 4
Public safety/emergency services	Degraded location, dispatch or communications capability for safety-critical response.	Risk 5
Energy system stability	Degraded timing-dependent grid monitoring, protection or control.	Risk 6
Adversarial/state denial	Intentional jamming, spoofing or electronic attack rather than natural/technical failure.	Risk 7
Space-weather multi-hazard	Simultaneous multi-system failure (PNT, power, satellites) from a single natural-hazard event.	Risk 8

This taxonomy is used consistently across Sections 4–5, the SDG cross-reference in Section 6, and the enterprise risk register in Section 7/Appendix D, so that a risk can be traced from its strategic root through to its SDG linkage and its enterprise manifestation using a single classification scheme. The seven source categories underpinning the evidence base are: UK government; US government; Australian government/research ecosystem; international/allied; academic/institutional; World Economic Forum; and insurance/catastrophe risk.

Appendix B. Full Longlist of Risks Considered

The eight risks ranked in Section 5 were selected from a broader candidate longlist. Risks below the corroboration threshold (fewer than two independent source categories) or judged to be sub-mechanisms of a retained risk rather than distinct risks, are listed here with the rationale for exclusion or consolidation, so that the Forum’s prioritisation logic remains auditable and revisable.

Table 7: Candidate risks considered

Candidate risk	Disposition	Rationale
Loss of maritime port crane/logistics automation	Consolidated into Risk 3	Sub-mechanism of multi-modal transport operability rather than a distinct failure mode.
Precision agriculture disruption	Retained only as SDG linkage (SDG 2, 15), not as a standalone national risk	Corroborated in only one source category at national-risk level; stronger as an SDG-mapping finding.
Autonomous vehicle/drone safety incidents	Consolidated into Risk 3 and Appendix C Risk 3	Treated as an enterprise/product-liability manifestation of transport safety risk rather than a separate national risk.
Undersea cable navigation/positioning for repair vessels	Below corroboration threshold	Single-source mention only; retained as a watch item for the next longlist refresh.
Financial market flash-crash triggered by timing corruption	Consolidated into Risk 4 and the enterprise register (Appendix C Risk 2)	Treated as a specific manifestation of telecoms/timing synchronisation failure rather than a distinct national risk category.
GNSS jamming as a driver of road traffic accidents	Consolidated into Risk 3	Corroborated but judged a sub-mechanism of transport safety/operability rather than distinct.

Candidate risk	Disposition	Rationale
Loss of satellite-based disaster/emergency alerting	Consolidated into Risk 5	Overlaps materially with emergency-services degradation; not separately quantifiable in available sources.
Direct kinetic/ASAT threats to GNSS satellites	Below corroboration threshold for this report	Primarily a defence/space-security topic outside this report's open-source civil-resilience scope; noted for possible future Forum work.

This longlist should be revisited as new sources emerge, and any newly-corroborated risk should be proposed for promotion into the Section 5 ranking with a stated rationale in the same format as this table.

Appendix C – 8 Strategic Risks in detail

C1. Risk 1 – Cascading Critical National Infrastructure Single Point of Failure

Summary

The central strategic risk for the UK is that GNSS has become a cross-cutting dependency – a potential single point of failure inside a “system of systems” – such that loss or corruption of PNT does not stay inside one sector but propagates through communications, energy, transport, emergency services, finance and government functions [4, 19]. The Blackett Review’s core diagnosis is that UK awareness of GNSS is “out of step with our actual dependence upon it”, that vulnerabilities to natural and ground-based interference (including malicious attack) are poorly understood in some sectors, and that insufficient protection reduces collective resilience. The 2025 National Risk Register states that satellite-derived PNT signals underpin banking and transportation as well as “almost all the UK’s critical national infrastructure (including energy, emergency services...)” [3].

Mechanism

GNSS provides weak, easily-interfered radio signals used for position and precise time. Many CNI systems take timing from GPS-disciplined oscillators without continuous independent verification. Failure or spoofing in one node (e.g. telecom synchronisation) degrades dependent sectors such as emergency dispatch, port operations and market connectivity. London Economics emphasises sector interdependence and that nearly all sectors depend on communications for information exchange [22].

UK policy implications

This risk is the rationale for the National PNT Office, cross-government PNT Crisis Plan, National Timing Centre, eLoran proposal, holdover clocks, and consideration of minimum resilient-PNT requirements for CNI [5, 19]. Advisory work should treat PNT as horizontal CNI resilience policy, not a space-sector specialism.

Cross-source corroboration

Source type	Corroboration
UK government	Blackett “system of systems” / single point of failure; NRR 2025 space-based services and GNSS failure risks; PNT Framework

Source type	Corroboration
US government	DHS National Risk Estimate: GPS as an invisible utility; cascading sector effects; EO 13905 on responsible use/resilience
Australia	FrontierSI: PNT “intrinsically interwoven” across market sectors; critical infrastructure resilience framing
World Economic Forum	“Disruptions to critical infrastructure” defined to include physical and digital infrastructure, including satellites
Insurance	Lloyd’s/Cambridge HELIOS: cascade from power/satellite failure into wider economy
Academic	Infrastructure interdependency/cascading-failure literature; GNSS interference as multi-sector threat

Quantitative indicators

- PNT judged vital to CNI functioning across UK sectors [19].
- NRR: recovery from GNSS/space-service disruption can take several days to several weeks depending on scenario; permanently damaged satellites can take years to replace [3].
- DHS judges long-term unaddressed GPS dependency as an increasing threat to national, homeland and economic security [23].

SDG cross-reference: this risk underlies the strong linkages to SDG 8, 9 and 11 (Section 6) since cascading CNI failure is the mechanism by which a PNT event becomes an economic-growth, infrastructure and city-resilience event simultaneously.

C2. Risk 2 – Severe Macroeconomic Disruption from GNSS Outage

Summary

A sustained UK GNSS outage would impose a large, rapid economic shock – measured in billions of pounds within hours to days – through lost gross value added, lost utility (efficiency/safety) benefits, transport friction, port/logistics delay, and emergency-service degradation [21, 23].

Mechanism

GNSS underpins navigation for road freight and personal travel, maritime operations, precision agriculture, surveying, and location-enabled emergency response. When the signal is unavailable, productivity and safety benefits reverse into delay, diversion, cancelled operations and higher operating cost. Because GNSS also supports timing for networks that enable commerce, second-order losses accumulate even where a sector has partial holdover.

UK quantitative picture

Estimate	Figure	Source
Annual UK benefits of GNSS (2023)	£13.62bn p.a.	GOV.UK PNT Overview
24-hour UK GNSS loss	£1.42bn	GOV.UK PNT Overview
7-day UK GNSS loss	£7.64bn	GOV.UK PNT Overview
5-day UK GNSS loss (2017 study)	£5.2bn (£1.7bn GVA + £3.5bn utility)	London Economics 2017; Blackett Review
Share of 5-day impacts: road / maritime / emergency+justice	37% / 21% / 30% (88% combined)	London Economics 2017
Earlier annual benefit monetisation (2017)	£6.7bn p.a.	London Economics 2017
US daily loss of GPS use	~USD 1bn/day	RTI GPS final report
US 30-day outage	~USD 30bn (up to ~USD 45bn in peak planting)	RTI International, 2019

UK Space restates the London Economics five-day figure and the RTI US comparators and notes a US nationwide disruption range of roughly USD 785–1,318 million per day in related literature synthesis [49].

UK policy implications

Economic-loss estimates support investment cases for the National Timing Centre, eLoran, receiver hardening and CNI minimum standards. They also support treating PNT outage as a macro-critical contingency in Cabinet Office/DSIT crisis planning, not only a technical telecoms issue. Advisers should stress that published figures are lower bounds for pure GNSS loss; multi-hazard events (space weather with power loss) produce far larger insurance-sector estimates (see Appendix D).

Cross-source corroboration

Source type	Corroboration
UK government / economic	London Economics 2017; GOV.UK 2023 update; Blackett citation of £5.2bn; UK Space resilient-PNT economics
US government / sponsored	RTI/NIST economic benefits and outage cost; EO 13905 economic-security framing
Australia	FrontierSI cites multi-jurisdiction economic studies of GNSS dependence
World Economic Forum	Economic downturn/supply-chain and critical-infrastructure disruption as amplifiers
Insurance	Extreme multi-hazard loss scenarios, orders of magnitude larger when power fails alongside GNSS

SDG cross-reference: the figures in this appendix are the primary evidence for the strong SDG 8 (Decent Work and Economic Growth) linkage set out in Section 6.

C3. Risk 3 – Multi-Modal Transport Safety and Operability Failure

Summary

Transport is among the most GNSS-exposed parts of the UK economy and CNI. A PNT outage or interference event can simultaneously degrade road navigation and logistics, maritime navigation and port operations, aviation PBN/approach support, and increasingly rail applications, creating safety risk, congestion, cancelled movements and supply-chain delay [4, 22].

Mechanism

- Road: mass consumer and commercial navigation and fleet management; journey-time and fuel-efficiency benefits reverse into delay and higher cost. London Economics attributes about £1.9bn (37%) of five-day UK outage impacts to road applications [21].
- Maritime: navigation, AIS-related functions, port approaches and offshore operations; London Economics attributes about £1.1bn (21%) of five-day impacts. The UK National PNT Office has supported Royal Institute of Navigation work on maritime GNSS jamming/spoofing impacts [19].
- Aviation: Blackett and CISA document operational dependence and real-world interference affecting aircraft; spoofing/jamming can force reversion to conventional procedures and reduce capacity, and confidence loss can outlast the physical event [4, 23, 50].
- Rail: growing GNSS use for traffic management and asset applications increases future exposure [4].

UK policy implications

DfT, CAA, the Maritime and Coastguard Agency and Network Rail need sectoral resilient-PNT requirements aligned to the national framework. Port and logistics continuity plans should assume multi-day GNSS degradation, consistent with NRR recovery windows. Autonomous and high-accuracy applications (future UK SBAS/PPP) raise the integrity bar further [19].

Cross-source corroboration

Source type	Corroboration
UK government	Blackett sector chapters; London Economics road/maritime dominance of losses; NRR aviation disruption under space weather; RIN maritime interference report

Source type	Corroboration
US government	DHS NRE Transportation Systems Sector; CISA interference advisories; GAO GPS disruption/interference work
Australia	FrontierSI automotive/maritime/aviation sector dependence
World Economic Forum	Critical infrastructure and supply-chain disruption pathways
Academic	Road jamming-detection literature; aviation spoofing/jamming impact studies

Quantitative indicators

- Road 37%, maritime 21% of UK five-day outage impacts [22].
- US RTI: major economic channel via port operations and supply-chain interruptions [51].
- NRR: severe space weather includes disruption to aviation alongside GNSS loss [3].
- Real-world corroboration: an estimated 38,500 vessels were affected by GPS jamming between April and November 2025 [6], and over 2,300 Ryanair flights plus dozens of British Airways and easyJet flights were affected by suspected jamming over the Baltic [7].

SDG cross-reference: this appendix is the primary evidence for the strong SDG 11 (Sustainable Cities and Communities) and SDG 14 (Life Below Water) linkages in Section 6.

C4. Risk 4 – Telecoms, digital infrastructure and trusted-time failure

Summary

UK telecoms and digital infrastructure use GNSS as a primary source of precise time and frequency synchronisation. That dependency now extends beyond network transport into data centres, virtualised compute environments, identity and access services, event logging, distributed transaction ordering and digital signing or trusted-timestamp functions that rely on coherent system time [4, 19, 21].

Mechanism

Operators commonly discipline clocks with GPS-disciplined oscillators. Holdover quality varies: DHS notes rubidium/caesium holdover on the order of about a month versus ovenised crystal oscillators on the order of about two days without GPS [23]. Blackett highlights nanosecond-to-microsecond timing requirements in modern networks and the evolution of interference and cyber threats. Spoofing is especially dangerous because it can deliver wrong time with high confidence, not merely a loss alarm [23, 52].

This dependency extends into virtualised and distributed IT estates. Hypervisors, hosts and guest systems require coherent time for clustered services, authentication, certificate infrastructure, event logging and forensic correlation; material clock divergence can disrupt security controls and impair reliable reconstruction of an incident [53, 54].

Digital-signing and trust services require trustworthy time to establish whether a signature was created during a certificate's validity period and, where necessary, before revocation. Timing disruption or corruption can therefore create disputes over signature validity, transaction sequencing and non-repudiation even if underlying services remain available [54]

UK policy implications

This is the core business case for a National Timing Centre delivering resilient, terrestrial, sovereign UTC(NPL)-traceable time, plus holdover clocks and resilient receiver chips in CNI [19, 55]. Ofcom/DSIT regulatory and standards levers – minimum synchronisation resilience, testing, and disclosure of GNSS dependence – are high-leverage. NRR cyber-telecom scenarios (millions of customers affected; 999/112 access risk) illustrate how communications failure, whether from cyber or from timing loss, becomes a national emergency [3].

Cross-source corroboration

Source type	Corroboration
UK government	Blackett telecom timing dependence; National Timing Centre programme; PNT Framework infrastructure resilience; NRR telecom CNI scenarios
US government	DHS NRE Communications Sector as central interdependency hub; CISA interference/PNT vulnerability products; EO 13905; DHS S&T best practices 2025
Australia	FrontierSI telecom sector adoption; CISC PNT factsheet
World Economic Forum	Critical infrastructure includes internet and telecommunications; cyber espionage/warfare ranked high on two-year outlook
Insurance / space	Satellite and space-weather work linking communications/GNSS degradation

Quantitative indicators

- DHS: crystal holdover ~2 days; high-quality atomic holdover ~1 month (indicative) [22, 23].
- UK economic studies assign relatively small direct telecom GVA loss under pure outage assumptions if holdover works – the strategic risk is cascade and integrity, not only first-order GVA [21].
- WEF 2023/5: cyber espionage and warfare ranked #5 on the two-year risk outlook; critical infrastructure disruption is defined to include telecoms and satellites [18]

SDG cross-reference: this appendix underlies the strong SDG 7 and SDG 9 linkages in Section 6, since grid and telecoms synchronisation share the same underlying timing-dependency mechanism.

C5. Risk 5 – Emergency Services and Public Safety Degradation

Summary

Emergency and justice services are among the highest-utility, highest-societal-stakes GNSS users in the UK. London Economics finds that loss of GNSS would impose about £1.5bn of impact on emergency and justice services over five days – roughly 30% of total estimated outage costs – driven largely by lost utility benefits from slower or less accurate location, dispatch and response [21].

Mechanism

GNSS supports caller location, vehicle automatic-location, navigation to incidents, and timing for emergency communications, including architectures historically linked to TETRA and successor systems. Blackett notes the scale of UK ambulance fleets and the inadequacy of coarse cell-ID location relative to desired 5–10m emergency accuracy. DHS analysis stresses emergency services’ dependence on communications networks that themselves depend on GPS timing, and on transport/energy as supporting sectors [4, 23]. Jamming is a dual problem: devices can deny GNSS and interfere with public-safety radio bands. During a multi-hazard event (space weather or hostile campaign), emergency demand rises just as location and communications degrade – a dangerous correlation.

UK policy implications

The Home Office, DHSC, blue-light services and justice agencies should be priority cohorts for resilient PNT (multi-constellation/multi-frequency receivers, non-GNSS location, hardened communications timing, exercised degraded-mode standard operating procedures). NRR links between telecom failure and inability to access 999/112 reinforce joint planning [3].

Cross-source corroboration

Source type	Corroboration
UK government	London Economics emergency/justice at 30% of costs; Blackett emergency services chapter; NRR emergency services dependence on space-based PNT
US government	DHS NRE Emergency Services Sector workshop findings
Australia	FrontierSI critical infrastructure/societal dependence framing
World Economic Forum	Critical infrastructure and societal stability under multi-risk stress

Source type	Corroboration
Academic	GNSS interference impacts on safety-of-life applications

Quantitative indicators

- £1.5bn / 30% of UK five-day GNSS-loss impacts fall on emergency and justice services [21].
- Public-safety-answering-point-related annual utility benefits of GNSS estimated at about £1.92bn in the same study (an order-of-magnitude indicator of value at risk).
- NRR: disruption of space-based services impacts emergency services among other CNI [3].

SDG cross-reference: this appendix contributes to the strong SDG 11 (Sustainable Cities and Communities) linkage and the weak/indirect SDG 16 (Peace, Justice and Strong Institutions).

C6. Risk 6 – Energy System Stability and Control Degradation

Summary

The energy sector’s current day-to-day dependence on GNSS is often assessed as lower than transport or emergency services for pure short outages, but strategic risk is rising because of timing-dependent wide-area monitoring and control (e.g. phasor measurement units), SCADA-related timing, and the dual-hit problem in which the same space-weather events that deny GNSS also stress high-voltage grids [3, 4, 23].

Mechanism

GNSS provides precise timestamps for synchrophasors and event reconstruction. DHS notes that as phasor measurement units move from monitoring toward control functions, vulnerability grows; intermittent jamming longer than about 15 seconds may lose time synchronisation in some configurations; sector subject-matter experts warned of a possible false sense of security because historical GPS problems were limited. Blackett identifies electricity transmission among timing-dependent CNI. NRR severe space weather explicitly pairs regional power disruptions with GNSS loss. Insurance and Cambridge risk models show that when power fails at scale, economic and insured losses dwarf pure GNSS-outage estimates, making energy–PNT coupling a systemic concern [4, 8, 23, 56].

UK policy implications

DESNZ, NESO/network operators and Ofgem should require resilient timing architectures (terrestrial UTC distribution, holdover, spoofing detection) for protection and control. Energy resilience planning must jointly scenario-test GNSS denial and geomagnetically-induced-current/space-weather power stress. PNT minimum standards for energy CNI fit the Framework’s infrastructure resilience strand [5].

Cross-source corroboration

Source type	Corroboration
UK government	Blackett energy/electricity timing; NRR severe space weather (power + GNSS); PNT Framework
US government	DHS NRE Energy Sector; CISA PNT vulnerability products; DHS S&T best practices
Australia	FrontierSI energy sector listed among GNSS-interwoven markets

Source type	Corroboration
World Economic Forum	Critical infrastructure includes energy; extreme weather/Earth-system risks on long-term horizon
Insurance	Lloyd's/Cambridge HELIOS power-outage cascade economics
Academic	Interdependent-infrastructure cascading-failure models

Quantitative indicators

- London Economics: energy direct monetised GNSS benefit is small, but impact is rated “low risk, but potentially significant” [22].
- Cambridge HELIOS (US-centric power scenarios): direct shock examples from USD 220bn to USD 1.2tn of US economic impact across severity variants; global supply-chain disruptions up to USD 2.7tn in the extreme variant [56].
- NRR: severe space weather lasting on the order of 1–2 weeks; GNSS recovery several days; some satellites non-recoverable [3].

SDG cross-reference: this appendix is the primary evidence for the strong SDG 7 (Affordable and Clean Energy) linkage in Section 6.

C7. Risk 7 – Adversarial PNT Denial and Hybrid/State Threat Escalation

Summary

Intentional interference – jamming (denial) and spoofing (deception) – converts PNT dependence into a national-security and hybrid-threat problem. Equipment is inexpensive and widely available; effects can be local (port, airport approach, city centre) or wide-area; spoofing can induce hazardous incorrect position/time without a clear “signal lost” alarm [19, 23, 50].

Mechanism

GNSS civilian signals are extremely low-power at the receiver and historically lacked strong civil authentication (Galileo OSNMA is a partial mitigation path in Europe). Threat actors range from privacy jammers and criminals to state electronic warfare. UK NRR explicitly includes state threat to PNT services, electronic attack on space systems, and malicious-attack variants on space infrastructure; mitigations cited include counter-jamming, interference detection and space domain awareness [3]. US Executive Order 13905 directs strengthening national resilience through responsible use of PNT services, recognising deliberate-disruption risk [57]. Australian resilient-PNT work similarly treats denial as a critical-infrastructure and sovereignty issue [58, 59].

WEF mapping: state-based armed conflict ranks among the top current global risks; cyber espionage and warfare ranks high on the two-year outlook; geoeconomic confrontation is elevated – all environments in which PNT denial is a known asymmetric tool [18]. Academic work continues to demonstrate practical spoofing/relay risks even against some authenticated designs [60].

UK policy implications

Treat electronic-warfare/PNT threats as a joint MOD–civil CNI problem. Priorities: interference monitoring and attribution; receiver standards (multi-frequency, multi-constellation, authentication-ready, anti-jam); legal/enforcement action against domestic jammers; an exercised PNT Crisis Plan; and sovereign complementary PNT (eLoran, National Timing Centre time, future options). Avoid over-reliance on any single foreign constellation even when multi-GNSS is used.

Cross-source corroboration

Source type	Corroboration
UK government	Blackett malicious interference; NRR state threat to PNT/electronic attack; PNT Framework crisis plan and resilient receivers; maritime interference work
US government	DHS NRE intentional jamming/spoofing scenarios; CISA interference insights; EO 13905; CISA PNT backup report
Australia	FrontierSI/Academy of Science resilient and sovereign PNT agendas
NATO / allied	STO electronic-warfare/collaborative PNT materials (threat environment)
World Economic Forum	Conflict, cyber and geoeconomic confrontation risk rankings
Academic	Extensive jamming/spoofing detection and attack literature

Quantitative / scenario indicators

- DHS scenario examples: low-power jammer ~500m ground radius; high-power and multi-jammer scenarios; spoofing inducing timing errors of hundreds of microseconds and position errors of tens of metres while receivers remain “confident” [23].
- Blackett: inexpensive jamming/spoofing equipment “readily available online”; ship-borne jammers can be very low power yet operationally disruptive [4, 19].
- NRR: restoration after some space/PNT attack scenarios could take up to several weeks [3].
- Real-world corroboration: an estimated 38,500 vessels affected by jamming across an eight-month 2025 window [6], and thousands of flights affected by suspected Baltic jamming [7].

SDG cross-reference: this risk is a cross-cutting amplifier of the strong SDG linkages (7, 8, 9, 11, 13, 14), since an adversarial denial event can trigger the same consequence classes as a natural or technical failure, only with less warning.

C8. Risk 8 – Space-Weather Multi-Hazard Catastrophe

Summary

Severe space weather is the clearest nationally registered, physically plausible pathway to simultaneous PNT loss and wider infrastructure stress. Unlike a pure local jammer, a major geomagnetic storm, solar energetic particle event or radio burst can degrade GNSS globally or regionally, damage or disable satellites, disrupt HF/satellite communications, affect aviation, and induce geomagnetically induced currents in power grids [3, 4, 8].

Mechanism

NRR lists coronal mass ejections, solar flares, solar radiation storms and solar radio bursts; impacts include regional power disruptions, GNSS loss/disruption, satcom/HF issues, aviation disruption, radiation dose increases, and ground digital-component effects. GNSS recovery may take several days; some satellites may be non-recoverable; overall severe events may last on the order of 1–2 weeks [3]. Blackett cites historical WAAS vertical-navigation outages of approximately 30 hours during the October 2003 geomagnetic storms. London Economics notes that space-weather outages are not independent of other failures – power and other satellite services may fail together [21].

Insurance-sector framing (systemic risk)

Source	Key figure / framing
Lloyd’s extreme space weather systemic scenario	Probability-weighted global economic loss USD 2.4tn over five years; range USD 1.2–9.1tn; expected loss USD 17bn; Europe ~USD 697bn modelled hit
Lloyd’s notes on GNSS economic role	GNSS alone estimated to support £320bn of UK GDP (as cited in Lloyd’s materials)
Cambridge HELIOS (AIG)	Multi-severity US-focused solar-storm scenarios with very large direct and supply-chain losses; insurance-loss examples USD 55–334bn across variants
Lloyd’s 360 Space Weather	Classic insurance-market education on cascade from space weather into terrestrial critical systems

WEF mapping: “non-weather-related natural disasters” explicitly includes geomagnetic storms in the WEF taxonomy; “disruptions to critical infrastructure” includes satellites; extreme weather and Earth-system risks dominate long-term rankings – space weather sits at the intersection of natural hazard and technological fragility [18, 61].

UK policy implications

Space weather is already on the NRR – the advisory task is to ensure PNT-specific mitigations (National Timing Centre, holdover, eLoran, multi-constellation, crisis plan) are integrated with energy grid resilience, aviation procedures, and satellite operations. Insurance and regulated-firm stress tests should include combined power + PNT + satellite-communications scenarios, not GNSS-only tabletop exercises. Sovereign terrestrial timing is a hedge precisely because the space segment and ionosphere are co-stressed in this risk class.

Cross-source corroboration

Source type	Corroboration
UK government	NRR severe space weather (explicit GNSS impacts); Blackett space-weather vulnerability; PNT Overview threat list
US government	DHS NRE naturally occurring disruptions (space weather); historical WAAS/ionosphere cases
Australia	FrontierSI references solar-storm power-disruption historical analogues
World Economic Forum	Geomagnetic storms in natural-disaster taxonomy; satellite-inclusive critical infrastructure
Insurance	Lloyd's systemic scenario; Cambridge HELIOS; Swiss Re satellite risk context
Academic / technical	Ionospheric scintillation and GNSS degradation research

SDG cross-reference: this appendix underlies the strong SDG 13 (Climate Action) linkage in Section 6 given the shared space-weather and satellite-monitoring pathway, and reinforces SDG 7, 9 and 14 through its power, infrastructure and maritime consequence classes.

Appendix D. Business Risk Register and Insurance/Liability Detail

Purpose

This appendix provides the full detail underlying Section 7 which reframes the national-level risk picture in Sections 4–5 for an individual, generic commercial business, using the financial-services sector (Section 7.1) as the illustrative exemplar while retaining a fully generic five-risk register applicable to any sector.

D1 Methodology and frameworks applied

Three complementary lenses are applied. First, resilience engineering, which models resilience as a function of time (Plan/Prepare → Absorb → Recover → Adapt) and space (Physical, Information, Cognitive and Social domains), and explicitly distinguishes resilience thinking – threat-agnostic, focused on performing well during and recovering quickly from disruption – from conventional threat-by-threat risk management [2].

This is the appropriate lens for PNT loss because the causes of disruption are diverse (space weather, satellite fault, jamming, spoofing, receiver fault) but the consequence – sudden loss of positioning and/or timing – is common across causes.

Second, UK business continuity and corporate governance practice: ISO 22301 Clause 8.2 (Business Impact Analysis) and 8.3 (continuity strategy) [10]; BS 65000, the UK organisational-resilience code of practice, which defines “essential outcomes” whose loss would cause significant, hard-to-remedy harm [62]; Cabinet Office business continuity management guidance [30]; and the FCA/PRA operational resilience regime, under which a direct review of Policy Statement PS21/3 found no explicit reference to GNSS, GPS or PNT anywhere in its text [1] – a regulatory blind spot that shifts the burden onto individual firms and boards to self-identify the dependency.

Third, strategic company risk register conventions: COSO ERM 2017, ISO 31000:2018, the UK Corporate Governance Code 2024 Principle O and Provisions 28/29, requiring boards to conduct a robust assessment of principal and emerging risks, and section 172 of the Companies Act 2006, the statutory director duty to have regard to the likely long-term consequences of decisions [13–16].

Risk scoring in the register below follows standard UK convention: Likelihood and Impact each scored 1 (Rare/Negligible) to 5 (Almost Certain/Catastrophic), Risk Score = Likelihood × Impact (maximum 25), illustrative and generic – an individual business should recalibrate against its own GNSS-dependency profile and risk-appetite statement.

The four resilience domains applied to enterprise PNT risk

Domain	Definition	PNT-loss relevance for a business
Physical	Sensors, facilities, equipment, system states and capabilities	Vehicles, plant, machinery, timestamping hardware, GNSS receivers, holdover clocks
Information	Creation, manipulation and storage of data	Positional/timing data feeding logistics systems, transaction records, telemetry, timestamps
Cognitive	Understanding, mental models, preconceptions, biases and values	Staff over-trust in GNSS accuracy; absence of “GNSS could be wrong” in operating procedures
Social	Interaction, collaboration and self-synchronisation between individuals and entities	Coordination with suppliers, customers, regulators and emergency services during disruption

This stage × domain structure is used as an analytical checklist for each of the five risks below rather than a literal matrix and is returned to explicitly in the Prepare/Absorb/Recover/Adapt checklist at the end of this appendix [2].

D2 The five strategic risks to a generic business – full register

Risk B1 – Supply Chain, Logistics and Operational Continuity Disruption

Field	Detail
Category	Operational / Strategic
Cause	Jamming, spoofing, satellite/constellation fault, or space weather degrades or removes GNSS positioning/timing signals
Event	Fleet tracking, route optimisation, port/rail scheduling, warehouse automation and just-in-time inbound logistics lose accurate position or time reference
Impact	Missed delivery windows, halted production lines dependent on JIT inputs, demurrage and service-credit penalties, inventory/stock-out costs
Inherent likelihood × impact × score	3 (Possible) × 4 (Major) = 12
Typical existing controls	Telematics with GNSS as sole position source; limited driver training on non-GNSS navigation; single-supplier GNSS chipsets

Field	Detail
Residual risk (typical current planning)	Often unchanged – most businesses have not tested a PNT-specific Business Impact Analysis scenario
Mitigation actions	Multi-constellation/multi-GNSS receivers; dead-reckoning/inertial backstop in fleet systems; contractual GNSS-outage clauses with logistics providers; BIA-derived Maximum Tolerable Period of Disruption for each PNT-dependent process
Owner	Chief Operating Officer / Head of Supply Chain

For most businesses, PNT loss first manifests as a logistics and operations problem, not an IT problem. GPS jamming affected an estimated 38,500 vessels between April and November 2025, concentrated in the Black Sea, Baltic and Persian Gulf [6], and commercial aviation reporting recorded over 2,300 Ryanair flights and dozens of British Airways and easyJet flights affected by suspected jamming over the Baltic in a single period [7]. The UK Government’s own economic impact assessment finds that 87.6% of the loss from a UK-wide GNSS outage would fall on emergency services, maritime and road transport [22] – sectors that are supplier-side dependencies for almost every other business.

Resilience domain view: Physical – vehicles/plant lose accurate positioning; Information – tracking and ERP/WMS systems ingest false or stale location data; Cognitive – staff and automated systems may not immediately recognise degraded data as erroneous, since “silent” GNSS error is often worse than an obvious total outage; Social – coordination with hauliers, ports and customers breaks down if none has a shared contingency protocol.

BCP linkage: this is squarely an ISO 22301 Clause 8.2 (BIA) and 8.3 (continuity strategy) exercise – define the Maximum Tolerable Period of Disruption for each PNT-dependent logistics process and pre-agree fallback procedures before disruption occurs [10, 63].

Risk B2 – Financial Transaction Integrity and Regulatory Compliance Failure

Field	Detail
Category	Compliance / Financial
Cause	Loss or spoofing of GNSS-disciplined timing signals used for transaction timestamping and clock synchronisation

Field	Detail
Event	Trade execution, settlement, ATM/payments network timing, or MiFID II RTS 25 clock-synchronisation obligations are breached or degraded
Impact	Mis-timed or unreconcilable trades, payment network disruption, breach of FCA impact tolerance for an important business service, regulatory enforcement, reputational damage
Inherent likelihood × impact × score	2–3 (Unlikely–Possible) × 4–5 (Major–Catastrophic) = 8–15
Typical existing controls	GNSS-disciplined clocks with limited or untested holdover; generic (not PNT-specific) third-party dependency mapping under FCA operational resilience rules
Residual risk	Elevated – FCA/PRA guidance does not name GNSS/PNT, so many firms have not mapped this dependency explicitly
Mitigation actions	Holdover-capable atomic/OCXO clocks at critical sites; explicit inclusion of GNSS/PNT in “important business service” dependency mapping; regular impact-tolerance testing against a PNT-loss scenario
Owner	Chief Financial Officer / Chief Risk Officer / Head of Regulatory Compliance

GNSS-derived UTC traceability underpins the clock-synchronisation requirements financial firms rely on for order timestamping (MiFID II RTS 25) and settlement. Under FCA Policy Statement PS21/3, regulated firms must identify “important business services,” set impact tolerances for disruption, and map underlying dependencies, including third parties [1]. The FCA and Bank of England have separately opened work on Critical Third Parties to the financial sector [32] – a category GNSS arguably belongs in, even though it is not yet named as such.

Resilience domain view: Information dominates (data/timestamp integrity), but cognitive factors matter too – a firm’s compliance and risk functions may not have considered GNSS an “important business service” dependency precisely because the regulator’s own guidance is silent on it.

BCP linkage: direct application of ISO 22301 Clause 8.2.3 (risk assessment) combined with FCA impact-tolerance testing [1, 10]; BS 65000’s “essential outcomes” concept is a useful reframing tool for compliance teams to escalate this internally [62].

Risk B3 – Safety-Critical Operations and Third-Party/Product Liability Exposure

Field	Detail
Category	Operational / Legal / Safety
Cause	GNSS spoofing or degraded accuracy feeds incorrect positional data into a safety-critical process or product
Event	Maritime pilotage, construction/surveying setting-out, autonomous vehicle or drone navigation, or GNSS-guided industrial plant acts on false position data
Impact	Personal injury, property damage, professional negligence claims, product liability claims, regulatory investigation, loss of licence to operate
Inherent likelihood × impact × score	2 (Unlikely) per incident, rising with automation × 5 (Catastrophic) where safety is engaged = 10
Typical existing controls	Sole reliance on GNSS positioning in operating procedures; limited crew/operator training on independent verification
Residual risk	Significant – demonstrated by real incidents (below)
Mitigation actions	Mandatory independent position verification for safety-critical tasks; anti-spoofing detection in GNSS receivers; design standards requiring graceful degradation rather than silent failure; adequate PI/product liability cover matched to GNSS-dependency profile
Owner	Chief Operating Officer / Head of HSE / Chief Engineer

This risk is not hypothetical. The Australian Transport Safety Bureau investigated a bulk carrier that came within 200 metres of grounding on the Great Barrier Reef after one of its GPS units began outputting incorrect positional data mid-pilotage, compounded by the pilot's sole reliance on GPS and failure to cross-check with an independent portable pilot unit [64]. RICS-regulated surveying firms – mandated to carry professional indemnity cover scaling with turnover – face comparable exposure where GNSS spoofing or error corrupts boundary, levelling or setting-out data, with claims for residential-scale errors typically settling at £10,000–£100,000 [40]. For manufacturers of autonomous vehicles, drones and GNSS-reliant industrial equipment, legal scholarship notes liability regimes are moving toward strict product liability combined with cybersecurity compliance requirements [41, 42].

Resilience domain view: Cognitive is decisive – the ATSB case turned on operator over-trust in a single GNSS source rather than a lack of alternative bridge technology. Physical and Information domains are secondary contributors; Social matters in the post-incident regulator, insurer and public-communication phase.

BCP and insurance crossover: this risk sits at the direct intersection of operational resilience (ISO 22301 Clause 8.3, “graceful degradation” design) and the professional indemnity/product liability insurance gap analysed below [10].

Risk B4 – Digital Infrastructure, Network Synchronisation, Trusted time, and Cyber-Attribution Disruption

Field	Detail
Category	Operational / Technology
Cause	Deliberate jamming/spoofing or natural GNSS signal loss disrupts GNSS-disciplined network timing (telecoms, data centres, point-of-sale, cloud infrastructure)
Event	Network synchronisation drifts or fails; downstream systems relying on accurate timestamps (logging, transaction processing, security certificates) degrade or fail
Impact	Service outage, data integrity loss, mischaracterisation of the event for insurance purposes (natural vs malicious), extended recovery due to unclear internal ownership (IT vs OT vs facilities)
Inherent likelihood × impact × score	3 (Possible) × 4 (Major) = 12
Typical existing controls	GNSS-disciplined network time servers without terrestrial backup; cyber incident response plans that do not cover RF/electronic-warfare-style interference
Residual risk	Elevated by classification ambiguity (see Insurance Aspects, below)
Mitigation actions	Terrestrial timing backup (NTP hierarchies independent of GNSS, holdover oscillators); explicit inclusion of GNSS/RF interference scenarios in cyber incident response and BCM plans; advance clarity on which insurance policy would respond
Owner	Chief Technology Officer / Chief Information Security Officer / Head of IT Infrastructure

GNSS-disciplined clocks are a common, often invisible, dependency of telecoms network synchronisation, data-centre operations and cloud/edge infrastructure. The CRO Forum representing Chief Risk Officers of major European (re)insurers, states that a GPS satellite failure could significantly affect banking transaction timestamping, aviation and maritime navigation, and telecommunications network synchronisation [9], citing the February 2022 Viasat KA-SAT cyberattack (attributed to Russian military intelligence) as the paradigm case of cross-border, cross-sector cascading impact from satellite-linked disruption.

This risk carries a distinctive complication: classification ambiguity. Whether a GNSS disruption is treated as a natural event, an accident, or a cyber-attack materially changes which insurance policy responds, and whether war/state-backed-attack exclusions apply (see Insurance Aspects, below). Resilience domain view: Information and Physical domains dominate, but Social and Cognitive domains govern the response, specifically, whether IT, OT, facilities and risk/insurance teams have a shared, pre-agreed protocol for triaging an ambiguous-cause disruption.

BCP linkage: ISO 22301 Clause 8.4 (business continuity plans and procedures) requires warning/communication procedures, precisely where a pre-agreed internal escalation and evidence-gathering protocol for an ambiguous GNSS event should sit [10].

Risk B5 – Governance Failure and Uninsured/Underinsured Loss from Inadequate Resilience Planning

Field	Detail
Category	Governance / Financial / Reputational
Cause	The board has not identified PNT/GNSS dependency as a principal or emerging risk, has not commissioned a Business Impact Analysis for it, and has not reviewed insurance coverage against it
Event	A PNT disruption event (any of Risks B1–B4) crystallises, and the business discovers simultaneously that it has no tested continuity response and no or inadequate insurance recovery
Impact	Direct financial loss uninsured or only partially insured; potential breach of Companies Act 2006 s.172 and Corporate Governance Code Provision 28 disclosure obligations; director and officer liability exposure; shareholder derivative claims; reputational damage from visible unpreparedness
Inherent likelihood × impact × score	3 (Possible) – reflects that this is the default state for most businesses today × 4–5 (Major–Catastrophic) = 12–15

Field	Detail
Typical existing controls	Generic enterprise risk management processes (COSO/ISO 31000-aligned) that have not yet specifically evaluated PNT/GNSS as a named risk
Residual risk	High by default until PNT is explicitly added to the risk register
Mitigation actions	Add PNT/GNSS dependency as an explicit principal or emerging risk in the board risk register; commission a PNT-specific BIA; review property, BI, cyber, PI and D&O policies against the gaps identified below; document the assessment for Corporate Governance Code Provision 28 purposes
Owner	Board / Chief Risk Officer / General Counsel

This fifth risk is a meta-risk: it is what converts Risks B1–B4 from a manageable operational event into a strategic, board-level crisis. The UK Corporate Governance Code 2024 Principle O and Provision 28 requires boards to carry out a “robust assessment” of principal and emerging risks and confirm this in the annual report [15]. Section 172(1)(a) of the Companies Act 2006 requires directors to have regard to the likely long-term consequences of their decisions [16], a duty that, by direct analogy with director-liability analysis in the climate-risk context, could expose directors to liability under s.172 if they fail to consider a foreseeable, material risk, or fail to consider it adequately [37]. ClientEarth v Shell – unsuccessful on permission grounds – nonetheless established the template mechanism, a section 260 derivative claim, by which a shareholder could in principle pursue directors who ignored a foreseeable, material, PNT-related risk that later crystallised into loss [39].

Resilience domain view: this risk is disproportionately a cognitive and social domain failure, a failure of organisational mental models and governance interaction, rather than a physical or information-system failure per se. It is also the clearest illustration of Linkov and Trump’s central argument that resilience is a pre-disruption discipline: the Plan/Prepare stage is where this risk is won or lost, since by the Absorb stage it is too late to discover the insurance gap [2].

D3 Insurance Aspects: Liabilities and Risks from Insufficient PNT Resilience Planning

This section addresses directly the question a board and risk committee most need answered: if the business has not planned adequately, what is at stake financially and legally when a PNT disruption occurs?

Property and Business Interruption Insurance – the Physical Damage Trigger Gap

Standard commercial “all risks” property policies and their attached business-interruption (BI) sections are triggered by loss “consequent upon DAMAGE to Property” – insured physical damage is required before a BI claim can be made at all [31]. A GNSS/PNT signal outage typically disrupts operations without physically damaging the policyholder’s own property and therefore falls outside this trigger; a Lloyd’s active underwriter has observed that non-damage business interruption (NDBI) cover “is not necessarily that common” and that knock-on effects on navigation/timing “are unlikely to be insured under an NDBI cover” absent a specific product [44]. Contingent Business Interruption (CBI), covering disruption caused by damage at a supplier’s premises, is subject to the same physical-damage precondition and would not respond to a jamming/spoofing event that degrades a supplier’s systems without physical damage [33]. NDBI products, pioneered by Swiss Re Corporate Solutions and offered through Lloyd’s capacity, remove the physical-damage precondition and can respond to a GNSS disruption[34], but remain bespoke rather than mass-market and must be actively sought and negotiated [35].

Liability if not planned for: the business bears the full, uninsured direct cost of the operational disruption identified in Risks B1 and B4.

Cyber Insurance – Classification Ambiguity Between “Natural” and “Malicious” PNT Loss

Whether GNSS jamming or spoofing falls within, or is excluded from, a cyber policy turns on a fact-specific test of malicious intent that is often extremely difficult to establish in the moment; industry commentary notes that cyber exclusions in marine policies typically bar coverage for losses caused by malicious cyber events, so if there is no malicious intent it should be covered, but if there is malicious intent it becomes questionable [6]. The CRO Forum states that cyber insurance policies typically exclude the exposure from satellites through an infrastructure exclusion, a “silent cyber”-style gap where GNSS/satellite-linked losses are neither clearly included nor clearly excluded [9]. War exclusions and state attribution compound the problem, since jamming/spoofing is disproportionately linked to state actors [65], and the London Market Association’s cyber war exclusion clauses were drafted generically for cyber-attacks with no

explicit reference to satellite or GNSS systems, leaving genuine uncertainty over whether jamming – a radio-frequency/electronic-warfare act rather than an IT intrusion – would even be characterised as a “cyber-attack” for these clauses [36].

Liability if not planned for: the business may discover, only after a loss, that its cyber policy neither clearly covers nor clearly excludes the event, creating protracted coverage disputes precisely when cash flow and recovery speed matter most.

Directors and Officers Liability

The UK’s resilience-statement reforms require many large companies to describe how principal risks are addressed, their likelihood, impact, time horizon and governance processes [66]. Legal analysis of director liability for foreseeable systemic risks, developed in the climate-risk context but directly transferable, identifies four liability pathways under s.172: acting in bad faith by ignoring the risk; overlooking it for genuinely ignorant reasons; failing to obtain or properly consider expert advice; or a defective decision-making process [15]. *ClientEarth v Shell* established the derivative-claim mechanism by which a shareholder could pursue directors for mismanaging a foreseeable, material risk, even though that particular claim did not succeed on permission grounds [39]. Critically, D&O insurance response is not guaranteed even if a claim is brought. Under the Insurance Act 2015 directors must make “a fair presentation of the risk” to D&O insurers at placement, and failing to disclose a known, material PNT dependency risk before placement could itself prejudice the policy’s later response [38].

Liability if not planned for: individual directors carry personal exposure to derivative and regulatory claims, and the D&O policy intended to protect them may itself be vulnerable to non-disclosure arguments precisely because the risk was foreseeable and undocumented.

Professional Indemnity and Product Liability

Professional indemnity (PI) insurance responds to financial loss caused by a professional’s negligent act, error or omission, including negligent reliance on inaccurate GNSS-derived positioning or timing data. RICS-regulated surveying firms must carry PI cover scaling with turnover, from £250,000 up to £1 million or more [40], and a GNSS spoofing or accuracy-degradation event causing an incorrect boundary, levelling or setting-out certification would typically be pursued against this cover. For manufacturers of autonomous vehicles, drones and GNSS-reliant industrial equipment, legal scholarship indicates liability regimes are converging on strict product liability combined with cybersecurity/anti-spoofing compliance expectations [39, 41], and the CRO Forum recommends insurers require alternative positioning technologies, redundant ground infrastructure and multi-constellation GNSS receivers as a precondition of favourable underwriting terms [9].

Liability if not planned for: professional and product liability claims arising from GNSS-driven errors fall on policies priced and underwritten without the insurer necessarily having assessed the business’s actual GNSS-dependency and mitigation posture, increasing both the probability of a coverage dispute and the likelihood of adverse renewal terms.

Regulatory and Contractual Liability

For regulated financial firms, breaching an FCA/PRA impact tolerance for an important business service because of unmanaged third-party GNSS dependency exposes the firm to supervisory action, and potentially enforcement, under the operational resilience regime [1]. For all businesses, conventional contract-law exposure arises through service-level agreements: logistics and manufacturing supply contracts typically specify accurate delivery timescales backed by service credits, and a PNT-driven routing/tracking failure causing missed delivery windows exposes the business to service-credit deductions, damages claims, and, for just-in-time manufacturing clients, consequential-loss claims where the client’s own production line stops as a result [43].

Liability if not planned for: regulatory enforcement risk for regulated firms, and uninsured contractual/consequential-loss exposure for all businesses with PNT-sensitive supply or delivery obligations.

The Insurer and Underwriter Perspective – What “Sufficient Planning” Actually Buys

Insurers and reinsurers already treat GNSS/PNT-linked disruption as a material and growing systemic exposure. Lloyd’s published a dedicated systemic risk scenario on extreme space weather in March 2025, modelling a probability-weighted \$2.4 trillion global economic loss over five years, ranging from \$1.2 trillion to \$9.1 trillion, and estimating the UK alone could suffer a \$113 billion loss because of its heavy reliance on GPS-style tracking systems [8, 67]. Swiss Re Institute’s SONAR emerging-risk reports have repeatedly tracked space weather and satellite/GNSS-linked risk [68], and Swiss Re’s analysis of satellite constellations further frames the growing systemic exposure to space infrastructure [45].

Source	Key figure / framing
Lloyd’s extreme space weather systemic scenario	Probability-weighted global economic loss \$2.4tn over five years; range \$1.2–\$9.1tn; UK loss estimated at \$113bn

Source	Key figure / framing
CRO Forum (European re/insurers)	Insurers “may incentivize” advanced security/redundancy with favourable terms or premium reductions; “price loadings” where standards are not met
GOV.UK / London Economics	Resilience improvements since 2017 have already reduced the modelled UK GNSS-outage impact by £1,171.1m; resilient PNT infrastructure could cut a 7-day outage loss by almost 50%

The consistent message from brokers and (re)insurers is that documented planning changes insurability and terms even where no formal rate card exists, while absent demonstrated mitigation, one Lloyd’s underwriter stated bluntly that “no insurer is going to sit there and add coverage for it without a premium... if exposed, it would actually be excluded because of the systemic nature” [44]. Bespoke affirmative products are emerging for buyers who proactively seek them, illustrated by dedicated maritime cyber products offering affirmative cover for cyber-related losses including malicious events and third-party errors [6].

The practical conclusion for a board is that the cost of inadequate PNT resilience planning is not simply the direct loss if disruption occurs – it is that direct loss, compounded by a high probability that standard insurance will not respond, further compounded by personal and corporate governance liability for having failed to address a reasonably foreseeable and increasingly well-documented risk, while businesses that have done the planning work are positioned to negotiate materially better terms.

D4 Applying the frameworks: a practical approach

Governance/standard requirement	What it requires	Recommended action for PNT/GNSS specifically
ISO 22301 Clause 8.2 (BIA and risk assessment)	Identify critical activities and the impact of their failure	Commission a PNT-specific Business Impact Analysis; define MTPD/RTO/RPO (holdover time) for each PNT-dependent process
ISO 22301 Clause 8.3 (continuity strategies)	Select and resource a response strategy	Multi-constellation receivers, terrestrial timing backup, non-GNSS operating procedures for safety-critical tasks
BS 65000 (essential outcomes, impact thresholds)	Identify services whose loss would cause significant, hard-to-remedy harm	Explicitly classify which “essential outcomes” depend on PNT; stress-test against a severe-but-plausible GNSS-loss scenario
FCA PS21/3 (regulated firms)	Map dependencies for important business services; set impact tolerances	Add GNSS/PNT explicitly to third-party/technology dependency maps, even though the FCA’s own guidance does not name it
UK Corporate Governance Code, Provision 28	Robust assessment and disclosure of principal/emerging risks	Add PNT/GNSS dependency to the board risk register as a principal or emerging risk, with documented mitigation
Companies Act 2006, s.172	Directors must have regard to long-term consequences	Ensure the board has considered, and can evidence having considered, PNT dependency and its foreseeable consequences
COSO ERM (Principle 7, risk appetite)	Define and apply risk appetite	Set an explicit risk appetite statement for PNT/GNSS dependency, distinct from generic IT/cyber risk appetite
Insurance programme review	–	Test each policy (property/BII, CBI, cyber, PI, product liability, D&O) against the PNT-loss scenarios above; commission bespoke NDBI or affirmative cover where gaps are found

Appendix E: References

- [1] Financial Conduct Authority. "PS21/3 Building Operational Resilience." Financial Conduct Authority. <https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience> (accessed 2026).
- [2] I. Linkov and B. D. Trump, "Risk, Systems and Decisions The Science and Practice of Resilience," ed. Switzerland: Springer, 2019.
- [3] HM Government, "National Risk Register 2025," HM Government, gov.uk, 2025. [Online]. Available: <https://www.gov.uk/government/publications/national-risk-register-2025>
- [4] Government Office for Science, "Satellite-derived Time and Position: A study of Critical dependencies," HM Government, London, 2018. [Online]. Available: <https://assets.publishing.service.gov.uk/media/5a82c84ced915d74e34038ab/satellite-derived-time-and-position-blackett-review.pdf>
- [5] (2023). *Framework for Greater PNT Resilience* [Online] Available: <https://questions-statements.parliament.uk/written-statements/detail/2023-10-18/hcws1073>
- [6] Claire Wilkinson. "Marine risks rise as GPS jamming spreads." Business Insurance. <https://www.businessinsurance.com/marine-risks-rise-as-gps-jamming-spreads/> (accessed 2026).
- [7] Gwyn Topham. "Thousands of Flights to and from Europe Affected by Suspected Russian Jamming." The Guardian. <https://www.theguardian.com/business/2024/apr/22/thousands-of-flights-to-and-from-europe-affected-by-suspected-russian-jamming> (accessed).
- [8] Lloyds, "Lloyd's Highlights Risk of Extreme Space Weather," ed, 2025.
- [9] The CRO Forum, "Understanding and mitigating the impacts of space related risks," 2025. [Online]. Available: <https://thecroforum.org/wp-content/uploads/2025/10/CRO-ERI-Space-Risk.pdf>
- [10] *22301: 2019 Security and resilience - Business continuity management systems - requirements*, ISO, iso.org, 2019. [Online]. Available: <https://www.iso.org/standard/75106.html>
- [11] Rick Cudworth, "A guide to BS 65000 - organisational resilience," in "A BSI executive Briefing," National Preparedness Commission, National Preparedness Commission, 2022. [Online]. Available: https://nationalpreparednesscommission.uk/wp-content/uploads/2022/09/BS_65000_Exec_brief.pdf
- [12] Bank of England, "Operational resilience: Impact tolerances for important business services," 2022. [Online]. Available: <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-22.pdf>
- [13] Institute of Risk Management, "From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks," Intsitute o Risk Management. [Online]. Available: <https://www.theirm.org/media/6885/irm-report-review-of-the-coso-erm-frameworks-v2.pdf>
- [14] *ISO 31000:2018 Risk management - guidelines*, ISO, iso.org, 2018. [Online]. Available: <https://www.iso.org/standard/65694.html>

- [15] Financial Reporting Council, "UK Corporate Governance Code 2024," Financial Reporting Council, 2024. [Online]. Available: <https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/uk-corporate-governance-code/>
- [16] *Companies Act 2006*, H. Government, 2006.
- [17] UNOOSA and European GNSS Agency (GSA), "European Global Navigation Satellite System and Copernicus: Supporting the Sustainable Development Goals. Building Blocks towards the 2030 Agenda," UNOOSA.org, 2018.
- [18] World Economic Forum, "The Global Risks Report 2023 18th Edition," World Economic Forum, Switzerland, 2023. [Online]. Available: <https://www.weforum.org/reports/global-risks-report-2023>
- [19] HM Government. "Positioning, Navigation and Timing: Overview." Department for Science, Innovation and Technology. <https://www.gov.uk/guidance/positioning-navigation-and-timing-overview> (accessed.
- [20] National Physical Laboratory, "The National Timing Centre (NTC), has today received investment from the Department for Science, Innovation and Technology," ed. npl.co.uk: National Physical Laboratory, 2026.
- [21] London Economics, "The Economic Impact on the UK of a disruption to GNSS," UK, 2021. [Online]. Available: https://assets.publishing.service.gov.uk/media/652eb0446b6bf000db7584e/20231018_London_Economics_Report_GNSS.pdf
- [22] London Economics, "Economic impact to the UK of a disruption to GNSS," InnovateUK, 2017. Accessed: April.
- [23] Department of Homeland Security, "National Risk Estimate: Risks to US Critical Infrastructure from GPS Disruptions," RNT Foundation, 2012. [Online]. Available: <https://rntfnd.org/wp-content/uploads/DHS-National-Risk-Estimate-GPS-Disruptions.pdf>
- [24] *Transforming our world: the 2030 Agenda for Sustainable Development*, U. Nations, 2015.
- [25] United Nations. "The 17 Goals." Department of Economic and Social Affairs. <https://sdgs.un.org/goals> (accessed 2026).
- [26] United Nations Office for Outer Space Affairs. "Space Supporting the Sustainable Development Goals." <https://www.unoosa.org/oosa/ourwork/space4sdgs/index.html> (accessed.
- [27] United Nations Office for Outer Space Affairs. "International Committee on Global Navigation Satellite Systems (ICG)." <https://www.unoosa.org/oosa/ourwork/icg/icg.html> (accessed.
- [28] European Space Agency, "ESA and the Sustainable Development Goals," 2018. [Online]. Available: https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Space_for_Earth/ESA_and_the_Sustainable_Development_Goals2.
- [29] Andy Proctor, "A structured approach to PNT Resilience and Assurance," PhD, Civil Engineering, Imperial College London, Unpublished (2025).
- [30] Cabinet Office. "Organisational Resilience Guidance for UK Government Departments, Agencies and Arm's Length Bodies (ALBs)." <https://www.gov.uk/government/publications/organisational-resilience-guidance-for-uk->

- [government-departments-agencies-and-arms-length-bodies/organisational-resilience-guidance-for-uk-government-departments-agencies-and-arms-length-bodies-albs-html](#) (accessed).
- [31] London & International Brokers Association, "Business Interruption Manual." [Online]. Available: <https://www.london-bia.org/lectures/LBIABIManual.pdf>
- [32] Financial Conduct Authority, "DP22/3: Operational resilience: critical third parties to the UK financial sector," ed, 2023.
- [33] Insurance information Institute. "Protecting your business against contingent business interruption and supply chain disruption." <https://www.iii.org/article/protecting-your-business-against-contingent-business-interruption-and-supply-chain-disruption> (accessed).
- [34] Swiss Re Corporate Solutions, "Non-physical Damage Business Interruption (NDBI)." [Online]. Available: https://higherlogicdownload.s3.amazonaws.com/RIMS/98329c33-d0ac-4661-b245-0765cf950581/UploadedFiles/0MtinnjtSoul5duh5XNT_NDBI%20Webinar%20Version%203.0%20Final.pdf
- [35] Strategic Risk Global, "Future of insurance: Non-damage business interruption." [Online]. Available: <https://www.strategic-risk-global.com/catastrophe-risk/future-of-insurance-non-damage-business-interruption/1434711.article>
- [36] Lloyds Market Association, "Bulletin: Cyber War Clauses." [Online]. Available: <https://lmalloyds.com/specialist-areas/underwriting/wordings/cyber-war-clauses/>
- [37] A. Stalker and A. Gordon, "Directors' Liability and Climate Risk: United Kingdom - Country Paper," Commonwealth Climate and Law institute, Smith School Oxford, 2018. [Online]. Available: <https://www.smithschool.ox.ac.uk/sites/default/files/2022-04/CCLI-UK-Paper-Final.pdf>
- [38] S. Holland, J. Sahota, and T. Edwards, "Directors & Officers Liability – Claims and Insurance in 2023." [Online]. Available: <https://gowlingwlg.com/en/insights-resources/articles/2023/directors-officers-liability>
- [39] C. Morgan and K. Hudson, "Shareholder Safeguards: A Practical Guide to Derivative Claims in UK Corporate Law." [Online]. Available: <https://www.charlesrussellspeechlys.com/en/insights/expert-insights/dispute-resolution/2025/shareholder-safeguards-a-practical-guide-to-derivative-claims-in-uk-corporate-law/>
- [40] Apex insurance Brokers Limited, "Surveyors Professional Indemnity Insurance – UK Guide 2026." [Online]. Available: <https://apexinsurancebrokers.co.uk/surveyors-pi-insurance-uk-guide-2026/>
- [41] M. Kubica, "Autonomous Vehicles and Liability Law," *American Journal of Comparative Law*, vol. 70, 2022, doi: <https://doi.org/10.1093/ajcl/avac015>.
- [42] N. AllahRakha, "Emerging Regulatory Countermeasures for Sensor Spoofing in Autonomous Vehicles," *Uzbek Journal of Law and Digital Policy*, vol. 3, no. 5, 2025.
- [43] K. Manship, "How can SLAs reduce supply chain risk?." [Online]. Available: <https://harperjames.co.uk/article/supply-chain-slas-performance-risk/>

- [44] R. Delaney, "Space Weather threat underlines gaps in risk quantification." [Online]. Available: <https://www.theinsurer.com/ti/news/space-weather-threat-underlines-gaps-in-risk-quantification-says-wtw-2025-03-14/>
- [45] Swiss Re Corporate Solutions, "New space, new dimensions, new challenges: How satellite constellations impact space risk." [Online]. Available: <https://www.swissre.com/dam/jcr:8bb6ac1d-a158-4b46-b32e-903ae5f89964/how-satellite-constellations-impact-space-risk.pdf>
- [46] IFRS integrated Reporting Examples Database, "Our Risk Management Framework: Risk heat map case study," Fresno PLC, 2012. [Online]. Available: <https://examples.integratedreporting.ifrs.org/fragments/risks-and-opportunities-19/>
- [47] M. Bartock *et al.*, "Foundational PNT Profile," National Institute of Standards and Technology, 2021. Accessed: Feb 11. [Online]. Available: <https://doi.org/10.6028/NIST.IR.8323>
- [48] Royal Institute of Navigation, "Three Stages To Resilient PNT." [Online]. Available: https://rin.org.uk/mpage/Resilient_PNT_Best_Practices
- [49] R. Flytkjaer and T. Goulding, "Economic benefits of resilient PNT in the UK " London Economics, London, 2022. [Online]. Available: https://www.ukspace.org/wp-content/uploads/2022/12/Economic-Benefits-of-Resilient-PNT-in-the-UK_Oct22.pdf
- [50] (2022). *CISA Insights: Global Positioning System interference*. [Online] Available: https://www.cisa.gov/sites/default/files/2023-02/CISA-Insights_GPS-Interference_508.pdf
- [51] A. C. O'Connor *et al.*, "Economic Benefits of the Global Positioning System (GPS) " in "RTI Report Number 0215471," RTI International, North Carolina, USA, 2019. [Online]. Available: https://www.nist.gov/system/files/documents/2020/02/06/gps_finalreport618.pdf
- [52] (2023). *Understanding Vulnerabilities of Positioning navigation and Timing*. [Online] Available: https://www.cisa.gov/sites/default/files/2023-04/fs_positioning-navigation-timing-vulnerabilities_508.pdf
- [53] Broadcom. "Use PTP for Time and Date Synchronization of Your ESXi Host." Broadcom. <https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/vcenter-and-host-management/host-configuration-host-management/synchronizing-clocks-on-the-vsphere-network-host-management/use-ntp-servers-for-time-and-date-synchronization-of-a-host-host-management.html> (accessed 2026).
- [54] Y.-S. Li and B. Van Eck, "Semiconductor Factory and Equipment Clock Synchronization for e-Manufacturing," National Institute of Standards and Technology, 2004 2004. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7184.pdf>
- [55] National Timing Centre (NTC). "National Timing Centre Programme." National Physical Laboratory. <https://www.npl.co.uk/ntc> (accessed).
- [56] E. Oughton *et al.*, "Helios Solar Storm Scenario," in "Cambridge Risk Framework Series," Centre for Risk Studies, University of Cambridge, 2016. [Online]. Available: <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/aig-helios-solar-storm-16-june.pdf>
- [57] White House, "Executive Order 13905: Strengthening National Resilience Through Responsible Use of PNT." [Online]. Available: <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order->

- [strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/](#)
- [58] J. Critchley-Marrows, E. Rubinov, P. Delaney, J. Lee, and A. Linossier, "A Time and a Place for Resilience: Building resilience into PNT services for Australia," FrontierSI, 2024. [Online]. Available: https://frontiersi.com.au/wp-content/uploads/2024/02/FrontierSI_ResilientPNT_Report.pdf
- [59] C. Rizos, M. Higgins, S. Choy, and S. McClusky, "National Committee for Space & Radio Sciences: Australia in Space: Space-based PNT." [Online]. Available: <https://science.org.au/sites/default/files/2025-11/pnt-final-wg-report.pdf>
- [60] M. Motallebighomi, H. Sathaye, M. Singh, and A. Ranganathan, "Cryptography Is Not Enough: Real-time Location Spoofing of Authenticated GNSS Signals," *ArXiv preprint*, 2022. [Online]. Available: <https://arxiv.org/pdf/2204.11641>.
- [61] M. Hapgood and A. Thomson, "Lloyds 360 Risk insight: Space Weather impacts and implications," Lloyds, Lloyds.com. [Online]. Available: https://assets.lloyds.com/media/ec9c7308-7420-4f1a-83c3-9653b1f00a4c/7311_Lloyds_360_Space%20Weather_03.pdf
- [62] *BS65000: Organizational resilience. Code of practice*, BS 65000:2022 - TC, British Standards Institute, bsigroup.org, 2022. [Online]. Available: <https://knowledge.bsigroup.com/products/organizational-resilience-code-of-practice>
- [63] Cabinet Office. "Resilience in society: infrastructure, communities and businesses." HM Government. <https://www.gov.uk/guidance/resilience-in-society-infrastructure-communities-and-businesses> (accessed).
- [64] Australian Transport Safety Bureau, "MO-2022-005: Pilotage competency assurance safety recommendation after near grounding," Australian Government, atsb.gov.au, 2024. [Online]. Available: <https://www.atsb.gov.au/news/2024/pilotage-competency-assurance-safety-recommendation-after-near-grounding>
- [65] Allianz Commercial, "Expert Risk Article: GPS Jamming and spoofing incidents cause concern." [Online]. Available: <https://commercial.allianz.com/news-and-insights/expert-risk-articles/gps-interference.html>
- [66] Department for Business and Trade. "New transparency over resilience and assurance for big business." HM Government. <https://www.gov.uk/government/publications/new-transparency-over-resilience-and-assurance-for-big-business> (accessed 2026).
- [67] M. Bow, "Solar Storm "would cost global economy \$2.4 trillion", " in *Daily Telegraph*, ed: telegraph.co.uk, 2025.
- [68] Swiss Re institute, "SONAR Emerging Risk Reports," Swiss Re, 2025. [Online]. Available: <https://www.swissre.com/institute/research/sonar/sonar2025.html>

Appendix F: Document administration

Item	Detail
Document title	Strategic and Enterprise Risks from Loss of PNT Services
Authored by	Andy Proctor
Version	1.0
Date	28 September 2026
Status	Published
Classification	Public – for release
Funded by	RethinkPNT Limited
Author detail	Andy Proctor is Managing Director of RethinkPNT, an independent UK consultancy specialising in space, PNT, quantum systems, systems engineering and resilience. A former UK Government investor and Technical Director at the UK Space Agency, he has led major defence and space capability programmes across space, ground and user segments, and brings expertise in PNT, satellite communications and resilient systems. He is a current Vice President and a Fellow of the Royal Institute of Navigation, Fellow of the Institution of Engineering and Technology, and a Chartered Engineer. He is also a resilience researcher at Imperial College London.
Acknowledgements	Air Vice Marshall (Rtd) Chris Moore CBE, for reviewing Richard Bowden, for reviewing