

When Products Fail – Beyond the Finished Product



Procurement and Supply Chain Management Made Simple.

Section Index

Section	Page
<i>Foreword</i>	4
<i>The Rise of the Online Marketplace</i>	5
<i>Who Is the Seller?</i>	5
<i>Unsafe Products Sold Directly from Overseas</i>	5
<i>The Emerging Responsibilities of Online Marketplaces</i>	6
<i>Removing Unsafe Listings Is Not Enough</i>	6
<i>From Platform to Product-Safety Gatekeeper</i>	7
<i>When the Product Is Part Physical, Part Digital</i>	7
<i>Can Software Make a Safe Product Unsafe?</i>	8
<i>Product Safety After the Point of Sale</i>	8
<i>Software Updates and Continuing Responsibility</i>	9
<i>Cybersecurity as a Product Safety Issue</i>	9
<i>AI-Enabled Products – A New Category of Risk</i>	10
<i>When AI Learns After the Product Has Been Sold</i>	10
<i>Who Is Liable When an Algorithm Causes Physical Harm?</i>	11
<i>Human Oversight and the Safe Design of AI-Enabled Products</i>	11
<i>The End of the ‘Finished Product’?</i>	12
<i>Contracts Cannot Make Regulatory Duties Disappear</i>	12
<i>Product Specifications – The First Line of Contractual Protection</i>	13
<i>Warranties and Compliance Obligations</i>	13
<i>Indemnities for Product Liability</i>	14
<i>Liability Caps and Exclusions</i>	15
<i>Insurance – Is the Supplier Actually Covered?</i>	16

Section	Page
<i>Flow-Down Obligations Through the Supply Chain</i>	16
<i>Audit and Inspection Rights</i>	17
<i>Records, Cooperation and Preservation of Evidence</i>	17
<i>Product Safety Begins Before the Purchase Order</i>	18
<i>Supplier Due Diligence for Product Safety</i>	18
<i>The Danger of Buying on Price Alone</i>	19
<i>Managing Product Changes and Substitutions</i>	19
<i>Counterfeit Components and Product Integrity</i>	20
<i>Monitoring Suppliers After Contract Award</i>	20
<i>Procurement's Role When a Safety Issue Emerges</i>	21
<i>Building Product Safety into Category and Supply Chain Strategy</i>	21
<i>From Reactive Liability to Preventative Responsibility</i>	22
<i>Data as a Product Safety Tool</i>	23
<i>AI for Product Safety – Both Risk and Solution</i>	23
<i>Global Products, Diverging Regulations</i>	24
<i>Will Liability Follow the Product Throughout Its Digital Life?</i>	25
<i>What Does Good Product Safety Governance Look Like?</i>	25
<i>Safety Cannot Be Outsourced</i>	26
<i>Summary – Designing Safety into the Supply Chain</i>	26
<i>Sources and Further Reading</i>	27

Foreword

Products no longer remain static from the moment they leave a factory. They are sold through global marketplaces, assembled from components drawn from multiple jurisdictions, altered through software updates and increasingly shaped by artificial intelligence. Responsibility therefore extends far beyond the traditional manufacturer, distributor and retailer. Modern product safety depends on understanding who designed, supplied, modified, marketed and supported the product throughout its entire commercial and operational life.

That shift has profound consequences for procurement and supply chain management. A purchaser may buy from a marketplace without knowing the real manufacturer, rely on certification that applies to a different factory, or accept a software-enabled product whose behaviour changes after deployment. Contracts can allocate financial consequences, but they cannot replace competent due diligence, effective traceability or statutory responsibility. Safety must be designed into sourcing, specification, supplier selection, monitoring and post-market response.

The regulatory environment is evolving accordingly. Online marketplaces are moving towards greater product-safety responsibility, cybersecurity is increasingly recognised as a physical safety issue, and software and AI are challenging the traditional concept of a finished product. Where functionality can change after sale, responsibility may also need to continue after sale. The emerging principle is continuing product-safety responsibility for organisations able to create, identify, or control safety-relevant change.

For procurement and supply chain leaders, one lesson emerges repeatedly: product safety cannot be outsourced simply because manufacturing, fulfilment, software development or distribution has been outsourced. Every organisation involved in the journey from design to end user exercises some degree of commercial control and, with it, some measure of responsibility. That principle is tested against UK and international evidence drawn from courts, regulators, insurers and manufacturers across both public and private markets.

The Rise of the Online Marketplace

Online marketplaces have transformed retail from a broadly linear manufacturer-importer-distributor-retailer chain into a network in which platform operators, third-party merchants, fulfilment providers and overseas producers may all participate in one transaction. Office for National Statistics data show internet sales accounted for 27.4% of Great Britain retail sales in 2025, against just 3.4% in 2007. That growth means controls designed around identifiable domestic traders increasingly fail to cover transactions assembled digitally across jurisdictions.

The difficulty is not that established product-safety concepts have disappeared, but that e-commerce can separate legal responsibility from the consumer's practical experience. A marketplace may advertise the product, rank the listing, process payment, arrange fulfilment and control seller access without itself being the contractual seller. At the same time, the manufacturer sits thousands of miles away.

Consumer behaviour reinforces the problem. OPSS research involving 2,073 UK marketplace users found that 26% took no steps to check product safety before buying the item examined, and only 16% looked for safety certifications or labels; among those who made no checks, 34% assumed the product was safe. Which? has separately found that shoppers assume a well-known platform has already screened sellers, trusting a star rating never designed to verify safety.

Who Is the Seller?

A consumer clicking "buy" may encounter five different roles: the manufacturer, an overseas merchant, the marketplace operator, a payment intermediary and a fulfilment provider. The named seller may not manufacture, import, store or dispatch the goods. UK legislation allocates duties by function, so identifying who placed a product on the market, or imported or supplied it, determines who must answer a regulator or face liability.

The Product Regulation and Metrology Act 2025 acknowledges that modern supply chains need broader regulatory reach. It defines an online marketplace as an internet-based service or feature facilitating the marketing of products in the United Kingdom. It permits future regulations to impose requirements on those controlling access to, or content on, such marketplaces. Those powers do not by themselves make every marketplace the seller; detailed duties depend on secondary legislation made under the Act.

The Government's 2026 product-safety consultation therefore proposed clearer accountability where the producer sits outside the United Kingdom. Its model would look first to a UK manufacturer, authorised representative or importer; where none exists, and a product is sold at a distance from outside the UK, the person making the offer to the UK customer could carry responsibility instead. For higher-risk products, the Government also consulted on possible UK-based responsible-person requirements.

Consumers do not always perceive these distinctions. OPSS reported in 2025/26 that almost half of respondents lacked a clear understanding of what an online marketplace is, while separate research found 59% regarded knowing a product's country of origin or seller location as important, rising to 80% for large domestic appliances. A procurement team buying chargers, tools or PPE through a platform should capture the seller's legal name and address at the point of order.

Unsafe Products Sold Directly from Overseas

Direct overseas selling can remove the domestic importer who traditionally acted as a regulatory choke point. Instead of a commercial importer buying a container, checking documentation and distributing stock, individual parcels may travel directly from a foreign seller to thousands of UK households. Enforcement authorities then face dispersed consignments, high transaction volumes, and sellers that may have no assets, premises, or personnel within UK jurisdiction.

Border intervention remains important, but its scale illustrates the challenge. OPSS, working alongside Border Force, reported that 2024/25 targeting covered consignments containing more than 14 million goods, with 2.63 million, or 19%, refused entry into the UK. At Felixstowe, joint work with Suffolk County Council trading standards resulted in 6,289 unsafe telescopic ladders detained for destruction, alongside 7,216 e-scooters and 857 unsafe pet-heating pads, all intercepted before reaching consumers.

The financial value of prevention is measurable. OPSS estimated that border activity in 2025/26 avoided around £81 million in detriment linked to unsafe products and approximately £209 million linked to non-compliant products, including potential injury and property damage. OPSS cautions that non-compliance does not always imply physical danger, but testing still found 81% of 2,260 targeted marketplace purchases non-compliant, and 90% of 620 sampled toys failed UK safety requirements.

The Emerging Responsibilities of Online Marketplaces

The Product Regulation and Metrology Act 2025 provides the legislative machinery for a more interventionist marketplace regime. Its powers expressly cover products marketed through online marketplaces, product information, monitoring, verification, complaints, record retention and cooperation with relevant authorities. The March 2026 product-safety consultation then proposed a duty requiring marketplaces to act with due care to prevent, identify and remove dangerous or non-compliant products, reflecting the control platforms already exercise over seller access and listings.

That proposed duty is more demanding than a notice-and-takedown model. The government suggested risk-based monitoring before products go live, checks against safety alerts, reports and recalls, and additional verification for higher-risk categories, so a marketplace might be expected to verify declarations of conformity or safety information before allowing a listing. The policy direction is preventative: systems should stop foreseeable non-compliance rather than merely react after regulators or consumers discover it.

Seller governance forms the second limb. The proposed consultation includes due diligence against repeat non-compliant sellers, including recognising multiple profiles, verifying and updating contact details, applying enhanced monitoring, and removing sellers who repeatedly breach product-safety rules. “Know your business” controls would move identity verification closer to standards already familiar from anti-money-laundering regimes, which matters where recall notices or evidence requests must reach an accountable person quickly rather than an unverified digital alias.

The evidence behind those proposals is striking, and does not rest on regulators alone. A Which? investigation cited by the Government listed an illegal, dangerous heater on Amazon, eBay, Etsy and TikTok Shop in 2024; after removal, Which? relisted an identical heater from the same seller on all four sites two months later. eBay, Etsy and TikTok Shop initially failed to identify the heater, and Amazon removed it only after three weeks.

Marketplace responsibilities are developing alongside stronger enforcement architecture. The companion 2026 consultation proposed consolidated enforcement powers and civil monetary penalties as an alternative to predominant reliance on prosecution, though it did not prescribe a single marketplace penalty figure. Existing connected-product law shows the scale of sanctions already available. Under the Product Security and Telecommunications Infrastructure Act 2022 (PSTI), OPSS may impose the greater of £10 million or 4% of qualifying worldwide revenue, plus £20,000 daily for continuing non-compliance.

Removing Unsafe Listings Is Not Enough

Removing one unsafe listing solves only the immediate visibility problem. A product can reappear under a new title, altered photograph, different category, fresh seller account or another marketplace entirely. The Government’s 2026 consultation expressly identified sellers creating new accounts, operating numerous profiles, and miscategorising products to evade

checks, so effective control depends on linking identities, products, and risk signals over time rather than simply deleting a webpage after a complaint arrives.

The distinction between enacted law and policy proposal remains essential throughout this discussion. The 2026 consultation closed on 23 June, and its marketplace due-care model should not be described as binding unless and until implementing regulations are made; Parliament's direction of travel is nevertheless clear, since the 2025 Act deliberately created powers to regulate marketplace controllers, and Government has stated that online sales should reach a footing comparable with bricks-and-mortar retail.

The latest Product Safety Database figures underline the scale of digital corrective action. In 2025/26, 594 recorded actions involved removal of a listing by an online marketplace, 15% of 3,986 corrective actions, yet 479 involved recalls from end users and 1,102 involved border rejections. A useful illustration is the unsafe carbon-monoxide alarms in the Government consultation: four marketplaces carried 149 listings for five unreliable models, and eBay alone recorded 1,311 sales across 42 listings.

Information sharing is therefore as important as removal. Platforms can identify purchasers, transaction dates, delivery addresses, seller relationships and linked listings at a scale unavailable to most manufacturers or trading standards teams, and the 2026 proposals envisage cooperation with authorities and access to marketplace interfaces for regulatory tools. Purchasers should likewise preserve invoices, screenshots, serial numbers and seller details rather than assume a listing stays accessible once a product is withdrawn.

From Platform to Product-Safety Gatekeeper

A marketplace is increasingly difficult to characterise as a passive noticeboard when it controls admission, search ranking, payment architecture, fulfilment options, advertising and seller removal. Those capabilities do not automatically create manufacturer or seller liability, but they provide real opportunities to prevent harm. The 2025 Act recognises that reality by permitting requirements on people controlling marketplace access or content, while the 2026 proposals seek to translate platform control into explicit due-care obligations.

Operational practice is already moving in that direction. OPSS reported in 2025/26 that it maintained engagement with Amazon, eBay, Fruugo, AliExpress, Meta and TikTok Shop, and removed tens of thousands of potentially non-compliant baby products from sale; some platforms also prohibited food-imitation products and standalone lithium-ion battery listings. In October 2025, an OPSS e-commerce briefing attracted 107 attendees from 48 organisations, including more than 30 marketplaces and 15 other e-commerce bodies.

Public expectation is shifting in parallel. OPSS found 39% of UK adults considered products bought online less safe than those bought in-store, while consumers often expected established marketplaces to police sellers regardless of the legal position. The likely destination is not that every platform becomes the manufacturer, but that marketplace governance becomes a distinct product-safety function, verifying sellers, screening higher-risk listings and assisting recalls wherever a digital intermediary controls access to millions of consumers.

When the Product Is Part Physical, Part Digital

Modern products increasingly combine hardware, embedded software, connectivity and remote services into one functioning system. A car may depend on extensive software code; an infusion pump can combine sensors, firmware, alarms and dose calculations; a smart lock relies on physical mechanics and network authentication. The safety question is no longer just whether casing, wiring or component tolerances were correct at manufacture, because digital behaviour now forms part of a product's safety-critical performance.

UK legislation has begun to recognise this hybrid character. The Product Regulation and Metrology Act 2025 defines the regulated "product" as a tangible item, but section 2 allows requirements concerning its components and confirms that intangible components include

software. This is a significant drafting choice: software need not be a freestanding physical product to affect the regulatory treatment of the hardware it is integrated into, particularly where that software changes the risk presented.

Consumer connectable products already sit within a separate cybersecurity regime. Since 29 April 2024, the PSTI Act 2022 and its 2023 Regulations have required in-scope manufacturers, importers and distributors to meet baseline security requirements, including banning universal default passwords and publishing minimum security-update periods, with important exclusions for medical devices and certain regulated vehicles. OPSS penalties can reach the greater of £10 million or 4% of qualifying worldwide revenue.

Medical technology demonstrates the highest-stakes version of this convergence. The MHRA notes that software itself can be a medical device and that adverse software events may cause indirect harm. More than 5.6 million people in the UK live with diabetes, many relying on continuous glucose monitors or insulin pumps that translate sensor data and programmed logic directly into clinical decisions, so a digital malfunction can affect treatment even when every physical component remains intact.

Can Software Make a Safe Product Unsafe?

Software can make a mechanically sound product unsafe by changing how it senses, warns, accelerates, doses, locks, heats or shuts down. Defects may arise from coding errors, corrupted data, configuration conflicts or an update that interacts unexpectedly with hardware. The MHRA gives a stark regulatory example: failure in radiotherapy-planning software can calculate an incorrect treatment dose, potentially causing under-treatment, excessive radiation, burns or disruption to a patient's cancer pathway.

Motor vehicles provide an equally clear illustration. UK recall R/2025/002 covered 45,929 Tesla Model 3 vehicles because the tyre-pressure-monitoring warning could fail to persist between drive cycles, reducing the warning of under-inflated tyres and increasing collision risk. The remedy did not require a replacement component: Tesla installed modified software through an over-the-air update, so a safety defect and its corrective action were both digital, despite the affected hazard being entirely physical.

Commercial exposure can spread across several suppliers at once. Hardware may come from one manufacturer, firmware from another developer, cloud functions from a service provider and configuration from an integrator, so establishing which contribution actually made a product unsafe is rarely straightforward. A purchaser commissioning an automated building system should treat software versions, patch responsibilities and change approval as specification issues, not matters resolved informally after something has gone wrong.

Product Safety After the Point of Sale

Traditional product-safety thinking assumed that, apart from wear, misuse or maintenance, a product leaving the factory remained substantially the same. Connected products challenge that assumption: features can be enabled remotely, algorithms recalibrated, cybersecurity protections patched and operating parameters altered months or years later. The point of sale is therefore no longer the only meaningful safety checkpoint, and post-market monitoring must consider what the product has become, not merely what was tested before launch.

The automotive sector already reflects this lifecycle reality. Vehicle Certification Agency guidance applies software-update requirements under the relevant vehicle type-approval framework, with staged application dates extending through 2026 and beyond, wherever manufacturers execute updates affecting type-approved characteristics after registration. The compliance object is consequently not just the original vehicle specification but controlled change over time, a logic increasingly relevant to machinery, medical devices and smart-home equipment as well.

For purchasers, continuing responsibility requires an asset record that includes software as well as hardware: model, serial number, firmware version, update status, support expiry,

known vulnerabilities and recall history. Public-sector estates and private operators can otherwise hold thousands of nominally identical devices that behave quite differently because update histories diverge, undermining any comfortable assumption that identical model numbers imply identical current behaviour, condition, or risk to the people using them.

Private fleet and asset-leasing operators face this challenge just as acutely as public bodies. A leasing company placing thousands of connected vans, forklifts or medical pumps with customers cannot treat handover as the end of its involvement if it retains any ability to push updates or monitor performance remotely, so continuing responsibility should attach to whoever keeps that practical control, not to whoever merely holds the original invoice.

Software Updates and Continuing Responsibility

A software update can improve security, correct defects or add functionality, yet the same mechanism can also create a new safety hazard. Responsibility depends on the regulatory regime, the contractual chain and who controlled the change. In consumer contracts, section 40 of the Consumer Rights Act 2015 applies quality, fitness and description requirements to digital content after permitted modification, so an update does not automatically escape the standards applicable when the content was first supplied.

For regulated medical devices, post-sale responsibility is particularly explicit. Great Britain's strengthened post-market surveillance rules apply to devices placed on the market from 16 June 2025 and require manufacturers to continually gather safety and performance information, investigate incidents, and take corrective action where risks emerge. MHRA guidance identifies software updates as a possible field safety corrective action, and the legal manufacturer remains responsible even where reporting tasks are delegated.

The automotive sector shows responsibility across the software lifecycle: UN Regulation 156 requires software-update management systems for relevant vehicles from 1 June 2026, and an insurer may restrict cover where an accident results from knowingly failing to install a necessary update. Practice confirms the pattern: in 2026 the MHRA published Field Safety Notices for products including Abbott's Merlin Patient Care System, and buyers should define who authorises and pays for changes.

Cybersecurity as a Product Safety Issue

Cybersecurity becomes a product-safety issue when digital compromise can alter physical behaviour. A malicious actor who gains control of a connected lock, heating appliance, vehicle, medical device, or industrial controller may create risks extending well beyond lost data. The National Cyber Security Centre warns that intrusion into operational technology can cause physical harm, environmental impact or disruption to essential services. Hence, safety engineering and cybersecurity overlap wherever software can command machinery, energy or access.

The scale of exposure is considerable, and not merely theoretical. Government evidence recorded an average of nine consumer-connectable products in a UK household in 2021, while cyberattack losses were estimated at more than £1 billion annually. A concrete illustration is the May 2017 WannaCry ransomware attack, which disrupted more than 80 NHS trusts and 8% of GP practices, cancelled over 19,000 appointments and diverted ambulances, at an estimated NHS cost of £92 million.

WannaCry did not involve consumer connectable products and falls outside the direct scope of the PSTI regime, but it demonstrates a wider safety principle: inadequate patching and cyber resilience can create serious operational and clinical consequences once digital infrastructure supports essential services. Government analysis has separately identified connected products with heating elements or locking mechanisms as capable of creating fire or physical-access risks if compromised, bringing cybersecurity and conventional product safety much closer together.

The PSTI regime has imposed baseline requirements on in-scope consumer connectable

products since 29 April 2024. Manufacturers must avoid universal default or easily guessable passwords, publish a vulnerability-reporting route and state the minimum security-update period, while importers and distributors carry additional compliance duties. OPSS can impose a maximum fixed penalty equal to the greater of £10 million or 4% of qualifying worldwide revenue, plus up to £20,000 for each continuing day of non-compliance.

Not every connected product sits within that regime. Medical devices, smart meters and certain vehicles are excluded because other frameworks apply, and many enterprise-only devices, such as office printers, cameras and building-entry systems, remain outside Part 1 of PSTI. The Government's 2026 response on enterprise device security warned that one vulnerable device can expose an organisation to data loss, service disruption, financial loss, or physical harm. Hence, procurement controls remain critical wherever statutory coverage differs.

AI-Enabled Products – A New Category of Risk

AI-enabled products introduce risks that conventional deterministic engineering does not fully capture. Their outputs can depend on probabilistic models, sensor inputs, changing data and contextual interpretation rather than a fixed sequence of programmed instructions. Government's 2026 product-safety consultation identifies automated decision-making and adaptive behaviour as emerging hazards across smart appliances, toys, home robots and industrial machinery, so the challenge is not simply whether hardware fails, but whether a functioning algorithm reaches an unsafe conclusion.

The Product Regulation and Metrology Act 2025 provides powers to regulate AI where it forms an intangible component of a physical product, but it does not create a general statutory code governing AI in isolation. Government policy remains sector-led, relying on regulators with relevant expertise, so an AI diagnostic tool, an automated vehicle and a household robot may share machine-learning techniques while presenting very different probabilities and routes of harm.

Healthcare already provides practical evidence of both the promise and the assurance burden. Panakeia Technologies' PANProfiler Colorectal system uses AI to analyse pathology slides and has been validated on more than 4,700 UK colorectal-cancer samples; around 44,100 people are diagnosed with colorectal cancer annually, while only 58% begin treatment within the NHS-recommended 62-day window, per MHRA's AI Airlock material. Faster AI-supported analysis may offer substantial benefit, but inaccurate classification could just as easily sway a clinical decision.

MHRA's second AI Airlock phase ran across seven technologies addressing clinical documentation, cancer diagnostics, eye disease and other applications, with participants including Panakeia Technologies, Eye2Gene, DeepX Health, Numan and NHS England's Federated Data Platform Safe Summarisation project. Their regulatory questions include validation, bias, post-market surveillance and controlled updates: product-safety disciplines translated into an environment where performance may vary by dataset, population, imaging system, software version and operational context.

When AI Learns After the Product Has Been Sold

The most difficult lifecycle question arises when an AI-enabled product does not remain behaviourally static. Government's 2026 consultation states that AI systems can evolve and adapt throughout operational life in ways that may be unpredictable or unforeseen at the point of use, then asks how regulation should account for AI that changes across the product's entire lifecycle. That framing challenges the traditional assumption that conformity can be assessed once against a stable, finished design.

Change can occur through retraining, recalibration, new datasets, model replacement or learning from operational experience, each of which may improve performance while also shifting error rates or creating new failure modes. Eye2Gene, participating in the MHRA AI

Airlock, identifies real-world issues including data drift, differences between retinal scanners, image quality and population variation, and has proposed a Predetermined Change Control Plan defining allowable updates, validation requirements and circumstances requiring further regulatory assessment.

Adaptive systems also complicate traceability in ways a conventional recall notice does not anticipate. Investigators examining an incident may need the model version, training data lineage, configuration, software dependencies, sensor state and update history that existed at the precise time of failure, since a serial number alone may no longer identify the relevant state. Procurement records should preserve digital configuration alongside physical asset identity, particularly where suppliers can alter models remotely.

Who Is Liable When an Algorithm Causes Physical Harm?

When an algorithm contributes to physical harm, liability may not rest with a single participant. The relevant route can include product liability, negligence, contract, sector-specific legislation or insurance, depending on the facts. Under Part I of the Consumer Protection Act 1987, liability for damage caused by a defective product can attach to specified producers and importers, while a supplier may become liable in defined circumstances if it fails to identify the responsible upstream party.

A documented real-world incident shows how quickly an algorithmic misjudgement can translate into physical injury. On 2 October 2023 in San Francisco, a Cruise self-driving taxi's software misclassified a collision, causing the vehicle to attempt to pull over rather than remain stationary; it then dragged a pedestrian, already knocked into its path by a separate human-driven car, roughly 20 feet, leaving her hospitalised for months. California's regulator suspended Cruise's operating permit within weeks.

The regulatory and financial consequences extended well beyond the algorithmic failure itself. The US National Highway Traffic Safety Administration fined Cruise \$1.5 million for incomplete crash disclosure, and the company separately admitted falsifying records in a federal investigation, accepting a further \$500,000 criminal penalty; combined settlements are reported to exceed \$10 million. The episode shows why investigators need model, sensor and decision-logic evidence, not just the vehicle, to establish what happened.

Software complicates causation further because the Product Regulation and Metrology Act 2025 treats software as a possible intangible component without replacing the underlying civil-liability framework. A physical product may incorporate software from one developer, sensors from another manufacturer, training data from a third source and integration by a systems contractor, so establishing which contribution made the product defective, or which conduct was negligent, requires the same forensic discipline as any engineering failure.

Automated vehicles show how UK legislation can allocate responsibility explicitly, rather than leaving it to be litigated each time afresh. The Automated Vehicles Act 2024 establishes a framework in which an authorised self-driving entity must ensure an authorised vehicle continues to satisfy the self-driving test. Under the Automated and Electric Vehicles Act 2018, first-instance liability for accidents while a vehicle drives itself sits with the insurer, with recovery rights against another party preserved.

Human Oversight and the Safe Design of AI-Enabled Products

Human oversight is valuable only when the human can understand the decision, detect abnormal behaviour and intervene before harm occurs. A nominal approval button offers weak protection when an operator lacks time, information, or authority to challenge an automated recommendation. Government's 2026 consultation identifies human oversight, data governance, documentation, standards, and quality assurance as potential safeguards for AI-enabled products, meaning effective oversight must be designed into the operating model rather than added as an afterthought.

The level of intervention should reflect consequence. An AI system recommending music does

not require the same controls as one influencing radiotherapy, vehicle movement or industrial machinery, and high-consequence products may require defined operating envelopes, confidence thresholds, independent sensors, emergency stops and safe shutdown states. The Automated Vehicles Act 2024 adopts an outcome-focused safety ambition, requiring that authorised automated vehicles achieve safety equivalent to, or higher than, careful and competent human drivers.

Healthcare provides a useful model for retaining professional judgement even as tools accelerate. Panakeia Technologies' PANProfiler can produce colorectal-cancer biomarker results within minutes, compared with laboratory processes that may take two to four weeks. Yet, it supports clinical decision-making rather than removing clinical accountability. Procurement should therefore test intended use carefully, because whether AI advises, prioritises, controls or acts autonomously materially changes the safeguards and assurance evidence a purchaser should demand before deployment.

Industrial robotics shows that the same questions extend well beyond healthcare and transport. In June 2026, the Health and Safety Executive announced work with the Regulatory Innovation Office, Automate UK and the Manufacturing Technology Centre to produce its first joint industry guidance for collaborative robots working alongside people. HSE research has also identified gaps in existing standards concerning AI, autonomous systems, cybersecurity and end-user interaction, reinforcing the need for risk assessment, protective stops and genuinely effective human intervention.

The End of the 'Finished Product'?

Connected products weaken the idea of a single moment when design ends, and responsibility becomes purely operational. A product may leave the factory compliant, receive new functionality six months later, change security configuration after a year and be recalibrated repeatedly thereafter. Government's 2026 consultation recognises this directly by asking how regulation should address AI that adapts throughout the product lifecycle, so the regulatory object increasingly resembles a changing system rather than an immutable manufactured item.

Medical-device regulation already contains elements of continuous product-safety responsibility. Great Britain's post-market surveillance rules require manufacturers to gather and analyse safety and performance information throughout the surveillance period, and higher-risk devices can require periodic safety update reports at least annually, with documentation retention generally at least 10 years, rising to 15 years for implantable devices. Responsibility therefore extends far beyond the invoice date and can continue after certification or production has ceased.

The commercial consequence is a shift from product acceptance to lifecycle assurance. Buyers may need to specify support periods, controlled-change procedures, vulnerability management, update testing, rollback capability, data retention and end-of-life arrangements alongside traditional dimensions, tolerances and warranties. A useful concept is continuous product-safety responsibility: accountability should remain with the organisations capable of creating, detecting or controlling safety-relevant change for as long as their decisions can materially alter the risk the product presents.

Contracts Cannot Make Regulatory Duties Disappear.

Contracts can allocate cost and recourse between organisations, but they cannot rewrite statutory obligations owed to the public. A manufacturer may obtain an indemnity from a component supplier, yet remain subject to duties imposed on manufacturers by product-safety legislation; a distributor cannot make an unsafe product lawful because its supplier promised compliance. OPSS guidance states that manufacturers, importers, distributors and sellers each carry responsibilities appropriate to their role when consumer products are supplied in the United Kingdom.

Consumer contracts are more restricted still. Section 31 of the Consumer Rights Act 2015 prevents traders from excluding or restricting core statutory liabilities concerning goods, including satisfactory quality, fitness for purpose and conformity with description, while section 47 provides corresponding protection for specified digital-content rights. Contract drafting therefore operates around mandatory law, not above it: indemnities, warranties and caps can determine recovery between commercial parties without depriving injured consumers of rights legislation makes non-excludable.

The distinction matters financially because the party answering the regulator or claimant may not ultimately bear the loss. A retailer might conduct a recall immediately, then pursue its supplier under warranty or indemnity; an insurer may compensate an automated-vehicle victim and later seek recovery from another responsible party. Good drafting therefore separates external legal responsibility from internal economic allocation, specifying defence control, notification, cooperation, evidence and contribution mechanisms without pretending statutory duties have been transferred.

Procurement teams should resist clauses stating simply that the supplier is “solely responsible” for product safety. Such wording may support contractual recourse but cannot guarantee that regulators, consumers or courts will ignore the purchaser’s own statutory role or negligence. The stronger approach maps legal responsibilities first and allocates financial exposure afterwards, a discipline that matters across public procurement worth about £385 billion annually and private chains where failures can outlive the contract.

Personal accountability provides a final reason contracts cannot make duties disappear. UK product-safety and health and safety legislation can expose individual directors and senior managers to prosecution where an offence is committed with their consent, connivance or neglect, regardless of how the company’s own contracts allocate financial responsibility internally. No indemnity clause between companies can extend to shield a named individual from that personal criminal exposure.

Product Specifications – The First Line of Contractual Protection

A product specification converts safety expectations into measurable contractual requirements before price and delivery pressures take over. It should identify applicable legislation, functional performance, operating environment, foreseeable misuse, materials, interfaces, software requirements, testing, marking, traceability and documentary evidence. Vague wording such as “industry standard” leaves unnecessary room for interpretation; where safety matters, the purchaser should objectively determine what compliance means, how it will be demonstrated, and what happens if the supplied product differs.

Public procurement law reinforces that discipline. Cabinet Office guidance under section 56 of the Procurement Act 2023 states that technical specifications may cover quality, performance, safety, dimensions, production methods, packaging, marking and labelling, and that contracting authorities should generally describe performance or functional requirements rather than unnecessarily prescribing a particular design. The guidance also permits certification or other evidence where standards are required, and accepts equivalent standards where the statutory conditions are met.

Grenfell provides the most sobering illustration of why specification and certification cannot be taken on trust. The Inquiry’s 2024 Phase 2 report found systematic dishonesty in testing and marketing products from Arconic, Celotex and Kingspan, contributing to 72 deaths and 58 accepted recommendations. A specification must therefore demand evidence connecting the tested configuration to the product actually supplied, including the exact test standard relied upon and disclosure of later changes to formulation or manufacturing site.

Warranties and Compliance Obligations

Contractual warranties turn representations about safety and compliance into enforceable promises between buyer and supplier. Typical provisions should address compliance with

applicable law, conformity with specification, required markings, valid certification, accuracy of technical documentation, absence of known safety defects and continuing notification of emerging risks. For connected products, warranties should also cover software support, authorised updates and cybersecurity obligations, so that the objective remains clear contractual recourse without confusing a warranty with independent regulatory approval.

Statutory implied terms may also operate alongside any negotiated warranty. In business sales, section 14 of the Sale of Goods Act 1979, as amended, implies terms concerning satisfactory quality and, where statutory conditions are met, fitness for a particular purpose, subject to applicable controls on exclusion. Consumer transactions are more protective: the Consumer Rights Act 2015 prevents traders from contracting out of core rights concerning satisfactory quality, fitness, description, and specified digital-content standards.

A compliance warranty should require evidence, not merely a declaration. OPSS guidance expects manufacturers and importers to demonstrate conformity with relevant regulations before placing products on the market, commonly through design controls, technical documentation, testing and conformity assessment. Depending on the product, UKCA or CE marking may be relevant, but marking alone should not be treated as independent proof of safety; purchasers should retain declarations, test reports, certificates, batch identifiers, and applicable assessment standards.

Warranties also need a lifecycle dimension. A supplier that warrants compliance only “on delivery” may leave uncertainty where a later software update, component substitution or regulatory change creates non-conformity, so better drafting requires ongoing notification, defect correction, regulatory cooperation, and disclosure of changes affecting certification or safety. Great Britain’s medical-device regime demonstrates the principle: manufacturers must continue monitoring devices after market placement and act on new evidence of unacceptable risk.

The strongest warranty package connects promise, evidence and remedy. Breach should trigger rights such as replacement, repair, re-performance, reimbursement of testing costs, suspension, recall cooperation and legally effective indemnified losses, sitting alongside insurance and liability provisions rather than replacing them. A supplier’s statement that a product “complies with all applicable laws” is a useful starting point, but assurance is materially stronger once the contract specifies supporting evidence and how long compliance must continue.

Indemnities for Product Liability

A product-liability indemnity is a contractual promise by one party to reimburse another for defined losses or liabilities. Properly drafted, it can shift the economic consequences of defective goods towards the supplier controlling design, manufacture or compliance, covering third-party claims, legal costs, regulatory response and recall expenditure. It does not transfer statutory responsibility owed to consumers or regulators, and remains only as valuable as the wording and the indemnifier’s financial strength.

Drafting precision matters because indemnities are interpreted according to their language and contractual context. A clause covering “claims arising from defective products” may not capture the purchaser’s investigation costs, replacement stock, business interruption or losses incurred before a third-party claim exists. Definitions should address defect, safety incident, recall, regulatory action and covered loss, while the contract should specify notification, defence control, settlement authority, mitigation and cooperation rather than leaving foreseeable exposure to implication.

Indemnities should be reconciled with liability caps rather than left ambiguous. A contract may cap general liability while staying silent on whether a product-safety indemnity sits inside or outside that cap, an ambiguity that can prove decisive after a major incident. Section 7 of the Consumer Protection Act 1987 prevents liability under Part I from being excluded against an injured claimant; an indemnity governs recourse between the parties, not that entitlement.

PPE Medpro illustrates the difference between a legal entitlement and actually recovering money. In October 2025, the High Court held that PPE Medpro breached its contract to supply 25 million sterile surgical gowns, ordering it to pay the Department of Health and Social Care approximately £122 million in damages; the company entered administration within days. A strong contractual right cannot eliminate counterparty-credit risk, which is why financial resilience and insurance matter alongside any indemnity.

Liability Caps and Exclusions

Liability caps are risk-allocation tools, but product safety tests their limits. Suppliers commonly seek a cap linked to annual charges, contract value or insurance, while purchasers may face injury claims, property damage, recall costs and disruption many times greater than the purchase price. A £500,000 supply contract can create exposure far beyond £500,000, so the real question is not merely whether a cap exists, but which liabilities it covers and whether it is legally effective.

English law does not permit every liability to be capped. Liability for death or personal injury from negligence cannot be excluded under the Unfair Contract Terms Act 1977, and other negligence restrictions must satisfy the reasonableness test. Section 7 of the Consumer Protection Act 1987 separately prevents liability under Part I from being limited or excluded by contract, so parties may allocate losses between themselves but cannot contract away an injured person's statutory claim.

The public sector must approach limits proportionately. Cabinet Office guidance under the Procurement Act 2023 requires conditions of participation on financial capacity and technical ability to be proportionate to the contract's nature, complexity and cost, and the Government's Mid-Tier Contract similarly requires authorities to set appropriate insurance types and amounts for their market. With public procurement exceeding £400 billion annually, poorly calibrated caps can expose taxpayers or unnecessarily exclude capable suppliers.

Product Recall Clauses

A product-recall clause should answer practical questions before an incident creates pressure: who must notify whom, within what period, who determines whether corrective action is required, and who communicates with regulators, customers and the media. UK product-safety guidance makes clear that manufacturers, importers, distributors and sellers carry responsibilities appropriate to their role, so a contract can organise cooperation between them without giving either party a veto over action that legislation or a regulator requires.

PAS 7100:2022, the British Standards Institution's government-backed code of practice for product recall, encourages businesses to prepare a product-safety incident plan before problems arise, addressing the roles, processes and responsibilities involved in corrective action. Contract clauses can reinforce that framework by requiring immediate incident escalation, traceability data, consumer-contact information, stock quarantine, investigation support and tested recall procedures, rather than attempting to invent them for the first time during an active crisis.

Haier's heat-pump tumble-dryer programme shows why recall governance needs continuing oversight rather than a single announcement. A corrective programme originally covered around 103,000 affected machines, but OPSS required Haier to halt the initial modification because the repair remained unsafe; an updated programme followed, with approximately 85,000 owners still requiring action in December 2025. A recall clause should therefore cover failed remedies and repeat interventions, not merely first contact with the customer.

Cost allocation should be equally explicit. Recoverable categories may include collection, transport, storage, destruction, repair, replacement, customer communications, call-centre capacity, expert testing and reasonable regulatory-response costs, with parties deciding in advance who controls public statements and settlements while preserving mandatory reporting obligations. OPSS publishes serious or high-risk products, recalls and modification

programmes through its Product Recalls and Alerts service, and commercial disagreement over cost should never delay measures needed to protect users.

Insurance – Is the Supplier Actually Covered?

A certificate stating “product liability insurance” does not establish that the purchaser is protected. Such insurance generally responds to legal liability for bodily injury or property damage caused by products manufactured, sold or supplied, and the ABI notes most UK businesses take cover for claims of between £1 million and £5 million. Product recall insurance addresses a different risk, covering the expense of recalling products that have caused, or may cause, injury.

Policy limits require the same scrutiny as contract limits. Purchasers should establish whether a limit applies per occurrence or the annual aggregate, whether defence costs erode it, and whether products liability shares an aggregate with other claims. Government templates illustrate this by letting authorities specify required limits and territorial scope; a £10 million certificate may provide materially less protection once prior claims and defence costs are considered.

The Lloyd’s Market Association’s Product Recall Committee reports an upward trend in both the number and cost of claims across the market, reflecting growing regulatory pressure, more complex global supply chains and rising consumer expectations. Insurers are responding by refining coverage terms and pushing clients towards more proactive risk management, which is itself a useful external check on whether a supplier’s own safety controls would satisfy an underwriter, not merely a procurement questionnaire.

Territorial and run-off provisions matter as much as headline limits. A UK supplier may sell components incorporated into equipment exported worldwide yet hold cover restricted to UK claims, while failures can emerge years after a supplier stops trading. Government contracting examples sometimes require insurance to continue for six years after expiry, and purchasers should check whether cover responds on an occurrence or claims-made basis, rather than assume a policy checked at signature still protects them.

Public procurement adds an important procedural qualification. Under section 22 of the Procurement Act 2023, contracting authorities cannot require contract-performance insurance before award as a condition of participation, though they may, where proportionate, require evidence that a supplier can obtain necessary cover and verify it is in place before commencement. This protects competition, particularly for SMEs, while still allowing buyers to require product-liability or other insurance justified by the contract’s actual risk profile.

Flow-Down Obligations Through the Supply Chain

A purchaser’s carefully drafted safety obligations lose value if critical work is performed two or three tiers below the contracting supplier without equivalent controls. Flow-down clauses require relevant obligations on product safety, specifications, testing, traceability, records, audit, cybersecurity, insurance and incident notification to be incorporated into subcontracts. The objective is not mechanical duplication of every main-contract term, but preserving controls wherever design decisions, manufacturing processes, component substitutions, or safety-critical services actually occur.

Government procurement guidance already uses this logic in other high-risk supply-chain areas. Procurement Policy Note 009 on modern slavery advises in-scope central government bodies, agencies, non-departmental public bodies, and NHS bodies to map supply chains, examine subcontractors, and use contract provisions requiring downstream due diligence. Product safety deserves comparable discipline: knowing the Tier 1 supplier is insufficient when another organisation controls a battery cell, fire barrier, sensor, or sterilisation process several tiers away.

Samsung’s global Galaxy Note7 recall remains the clearest illustration of how quickly a flow-down failure can escalate. Overheating and fires traced to battery cells led Samsung to recall

roughly 2.5 million devices in 2016, replacing them with units using a second supplier, whose cells then carried a separate defect; total costs were estimated at over \$5 billion. Neither battery tier was the phone's own manufacturing line, illustrating exactly the divergence flow-down clauses exist to prevent.

Effective flow-down also requires visibility and enforcement, not just a clause. The prime supplier should maintain an up-to-date supply-chain map, obtain approval for defined safety-critical changes, and remain responsible for subcontractor performance, with contractually supported audit rights, access to test reports, and traceability records. Without those mechanisms, a promise that subcontractors "will comply" becomes unverifiable, leaving the purchaser dependent on assurances from an organisation that cannot itself control the risk.

Audit and Inspection Rights

Audit rights convert product-safety assurances from promises into testable evidence. Depending on risk, a purchaser may need access to manufacturing sites, quality-management systems, test laboratories, technical files, batch records, calibration data, software-change controls and corrective-action records. Audits should be proportionate and targeted, not ritualistic, and Cabinet Office guidance confirms that, where proportionate under the Procurement Act 2023, evidence for conditions of participation can include certifications, site visits, audits and third-party verification.

The contract should define who may audit, how much notice is required, which sites and records are in scope, who pays and how confidential information is protected. Higher-risk arrangements may justify unannounced inspections, especially where announced visits could conceal working practices or non-conformity; government supply-chain guidance already contemplates clauses permitting unannounced or semi-announced visits and direct confidential engagement with workers, with drafting logic that transfers readily to product-safety audits.

Audit programmes should follow risk rather than the calendar. A low-risk standard product from a mature manufacturer may justify remote document review. At the same time, a safety-critical new design, overseas factory or unexplained component change may require physical inspection and independent testing. Findings should produce corrective-action plans with named owners and deadlines, followed by closure verification, because audit rights generating reports with no contractual consequence identify defects without reducing the probability of unsafe supply.

Records, Cooperation and Preservation of Evidence

Product-safety disputes are often won or lost on records created long before litigation begins. Useful evidence includes specifications, drawings, approvals, purchase orders, declarations of conformity, test reports, batch numbers, serial numbers, factory records, inspection results, software versions, complaints, photographs and correspondence. OPSS guidance requires manufacturers and importers to generate and retain relevant technical documentation, while sellers must keep records identifying suppliers so product origins can be traced years later if needed.

The PPE Medpro judgment offers a striking evidence lesson reaching well beyond pandemic procurement. The Department of Health and Social Care recovered approximately £122 million for the non-compliant gowns, but its separate claim for roughly £8.6 million in storage costs failed: the court found the spreadsheet poorly evidenced and the witness lacking real knowledge of the material. A cost may be commercially real yet legally unrecoverable if an organisation cannot prove how it arose.

Cooperation clauses should therefore activate immediately after a suspected incident, requiring preservation of potentially relevant documents and physical samples, identification of affected batches, access to personnel, assistance with regulators and insurers, and suspension of routine destruction policies. For digital products, preservation may require

model versions, logs, firmware, configuration data, and update histories. At the same time, parties should also address legal privilege and data-protection constraints so evidence is preserved lawfully rather than indiscriminately copied.

Retention periods should reflect product life, regulatory obligations and plausible claim periods rather than administrative convenience, since a safety defect may emerge only after warranties expire or suppliers merge, relocate or cease trading. Records should remain retrievable and intelligible, with clear responsibility for transfer on corporate change or contract exit. Traceability is not merely a recall tool: it lets investigators reconstruct what was supplied, by whom, and what changed before harm occurred.

Product Safety Begins Before the Purchase Order

Product safety begins when the requirement is conceived, not when a purchase order is raised. Early procurement decisions determine which hazards are designed out, which standards apply, what evidence suppliers must produce and how much commercial pressure the market must absorb. By contract award, many safety choices are already embedded, which is why government guidance places market engagement, specification, supplier selection and award within one integrated process, not as separate control points.

The scale of public purchasing makes early assurance particularly important. The Government Commercial Function's 2026–29 strategy states that the public sector spends more than £400 billion annually on goods and services, with the Function itself managing approximately £90 billion, while Treasury statistics show gross current procurement within Resource Departmental Expenditure Limit reached £179.1 billion in 2025/26. Even low failure rates can translate into substantial exposure when unsafe specifications or weak sourcing decisions repeat across programmes.

Preliminary market engagement can test whether safety requirements are technically achievable, whether recognised standards exist, how mature the supplier base is, and what testing lead times or costs apply, while also revealing where requirements unintentionally narrow competition. For public bodies, engagement must remain compatible with equal treatment and procurement law, enabling buyers to improve specifications before tender rather than discover after award that only one supplier can satisfy an unnecessary requirement.

OPSS data show why safety must be built into sourcing decisions rather than treated as a downstream compliance step. Fire and rescue services reported 211 fires involving e-bikes or e-scooters during 2024, causing eight fatalities, with 77 of 170 e-bike fires involving post-market conversions; London Fire Brigade alone submitted 175 of the notifications. Battery and charger compatibility and conversion controls therefore belong in specifications, not after a fire.

Private-sector purchasers face the same principle without the procedural framework of public procurement law. A retailer sourcing electrical appliances, a housing provider buying fire-safety equipment or a manufacturer purchasing lithium-ion batteries should consider foreseeable harm during category planning, addressing qualified suppliers, testing capacity, alternative supply and recall capability from the outset. Safety then stops being a late compliance check and becomes part of value, resilience and total cost from the very start of sourcing.

Supplier Due Diligence for Product Safety

Supplier due diligence asks whether the organisation behind the tender can reliably deliver safe products, not simply whether its documents look complete. Relevant enquiries may include regulatory history, recalls, enforcement action, technical competence, quality systems, manufacturing locations, testing capability, financial resilience and insurance. For public procurements, section 22 of the Procurement Act 2023 permits proportionate conditions addressing legal and financial capacity or technical ability, while the exclusions regime

separately addresses misconduct, insolvency and poor performance.

Financial resilience is a product-safety issue because recalls, remediation and litigation require money a struggling supplier may not have. Cabinet Office guidance identifies turnover, cash flow, debt-to-equity and liquidity as possible indicators of financial capacity, subject to proportionality, and the Act prevents authorities from demanding audited accounts from suppliers not otherwise legally required to produce them. Due diligence should consider whether a supplier could survive a plausible recall while still supporting affected customers.

Regulatory and performance history provide another stream of evidence. Schedule 7 to the Procurement Act 2023 includes discretionary exclusion grounds concerning professional misconduct, insolvency and sufficiently serious contractual breach or poor performance, subject to statutory tests and opportunities for suppliers to make representations. Product-safety buyers can also review OPSS recalls, enforcement notices, certification status, and comparable overseas information, recognising that a historic incident may show either persistent weakness or effective corrective learning since.

Market surveillance shows why seller assurances need independent verification, not acceptance at face value. OPSS tested 128 children's Halloween fancy-dress costumes bought from online marketplaces in 2024; more than 80% failed basic safety tests, with 28 of 128 failing flammability testing and 61 of 74 tested for cords and drawstrings failing outright. Buyers should examine manufacturer identity and test evidence, rather than treat marketplace availability itself as supplier due diligence.

The Danger of Buying on Price Alone

Price competition creates value only while the product remains capable, compliant and safe. Excessive downward pressure can encourage thinner materials, cheaper components, reduced inspection, shortened testing or substitution through unauthorised sources. However, none of this is inevitable, and low price is never itself evidence of poor quality. The risk arises when the commercial model leaves insufficient margin or time to perform required controls, while the buyer rewards savings without measuring how they were achieved.

The Procurement Act 2023 deliberately avoids equating value with lowest price. Cabinet Office guidance explains that the “most advantageous tender” need not be determined by lowest cost and that price does not have to take precedence over non-price factors, so for safety-critical goods, award criteria can give meaningful weight to technical assurance, testing, traceability and quality management where relevant and proportionate to the contract's actual risk.

Grenfell remains the starkest warning against letting economy outrun safety governance. The Inquiry found the refurbishment's failures were collective, and that manufacturers Arconic, Celotex and Kingspan engaged in dishonest conduct over product testing and marketing. At the same time, evidence before Parliament recorded value for money and appearance, not safety, as key drivers. Seventy-two people died; the lesson is not that cost reduction is unsafe, but that savings must never bypass competent technical scrutiny.

Managing Product Changes and Substitutions

A product approved at tender stage can become materially different during manufacture if a supplier changes resin, alloy, battery cell, microchip, adhesive, software library or production site. Some substitutions are harmless; others alter fire performance, electrical characteristics, durability or regulatory status. Contracts should therefore define safety-critical changes and prohibit implementation without prior written approval, supported by updated risk assessments, test evidence, certification and traceability wherever the proposed change could affect conformity or safe use.

Change control should extend beyond visible components. Moving production to another factory may introduce different machinery, quality systems or environmental conditions, while a firmware update can alter a connected product without any physical modification. Approved-

manufacturer lists, bills of materials, software baselines and controlled drawings give purchasers a reference configuration, and the supplier should flag departures from that baseline early enough for review, not present substitutions as an accomplished fact after delivery.

The Takata airbag scandal remains the starkest global warning about uncontrolled substitution. Takata's ammonium-nitrate propellant, without adequate moisture-proofing at some sites, caused inflators to rupture explosively; this ultimately led to more than 30 deaths and hundreds of injuries worldwide and triggered recalls of over 100 million airbags. Takata pleaded guilty to criminal wrongdoing and agreed to a \$1 billion US penalty before entering bankruptcy, showing how one substitution can outlast the company that made it.

A proportionate regime distinguishes routine change from safety-significant change. Commodity packaging may need simple notification, while a substituted flame retardant, pressure component, medical-device algorithm or lithium-ion cell may justify retesting and formal approval. The contract should also address emergency substitutions during shortages: pre-qualify alternative components and factories wherever possible, so continuity planning preserves both supply and the safety case on which the original purchase decision depended.

Counterfeit Components and Product Integrity

Counterfeit components pose a greater risk than simple trademark infringement, because an imitation may reproduce the appearance and part number of an approved component while omitting the materials, tolerances, or safety features that made the genuine item reliable. Grey-market goods add another layer: they may be genuine products diverted outside authorised distribution, leaving storage, provenance, warranty, or configuration uncertain. Product integrity therefore depends on traceability from approved source to installed component, not on appearance alone.

The scale of counterfeiting is substantial. The Intellectual Property Office reported that Border Force seized counterfeit articles with an estimated retail value exceeding £500 million between 2021 and 2023, and separate IPO research among 5,000 UK adults found 24% said they had knowingly bought counterfeit physical goods at some point, with 15% reporting doing so currently at least occasionally. Online purchasing has remained the dominant channel for that trend since the pandemic.

Electrical counterfeits demonstrate the safety consequences most vividly. A 2025 Redbridge Council prosecution concerned an estimated £750,000 counterfeit-electronics operation supplying products including laptop chargers, and OPSS-funded testing found that 48 of 50 samples posed serious risks, including electric shock and fire. In December 2025, OPSS separately reported a counterfeit Samsung USB-C charger presenting a high risk of electric shock because insulation clearances were inadequate; the import was rejected at the border before reaching sale.

Counterfeit risk is especially acute during shortages, when buyers or subcontractors may turn to brokers promising apparently equivalent parts outside authorised channels. Controls should include approved distributors, manufacturer verification, tamper-resistant identifiers, incoming inspection and batch-level traceability, quarantining safety-critical components wherever provenance cannot be demonstrated. A certificate from the immediate seller is not sufficient if the purchaser cannot reliably link that document to the physical item delivered.

Digital purchasing also requires disciplined catalogue control. In September 2026, OPSS reported an Amazon-listed charger for e-bikes, scooters, and hoverboards that posed a serious fire risk because the plug dimensions were non-compliant and its fuse was considered counterfeit and lacked ballast. The listing was removed, but purchasers may already possess the product, so procurement systems should preserve marketplace seller details and transaction records rather than relying on listings that can later disappear.

Monitoring Suppliers After Contract Award

Contract award marks the start of assurance, not its end. Supplier monitoring should test whether controls promised during competition continue to operate through production, delivery and use, using measures such as defect rates, failed inspections, safety incidents, overdue corrective actions, audit findings and unauthorised changes. The most useful indicators are leading ones that expose deteriorating control before an injury or recall, not measures that merely count failures after they occur.

For public contracts above £5 million, section 52 of the Procurement Act 2023 generally requires at least three key performance indicators unless performance cannot appropriately be assessed that way, subject to specified exceptions, and section 71 then requires assessing and publishing performance against those indicators at least once every twelve months and on termination. Safety-critical procurements can use that framework to make compliance and corrective-action closure visible rather than leaving them buried in operational meetings.

Monitoring should combine data with physical verification wherever possible. OPSS reported that five 2025/26 surveillance projects at major UK retailers tested 56 electrical products, including chargers, power banks and cables, prompting strengthened compliance controls across ranges totalling around 3.5 million items. Purchasers can adopt the same principle at contract level: analyse trends, sample products, audit records and escalate repeated non-conformity, so that supplier assurance becomes credible because reported performance is periodically tested against evidence.

Procurement's Role When a Safety Issue Emerges

When a credible safety issue emerges, procurement becomes as much a coordination function as a commercial one. The immediate priorities are to stop further exposure, identify affected products, preserve evidence and bring together technical, legal, operational, communications and insurance stakeholders. The supplier should be formally notified under the contract, with relevant rights reserved, and further deliveries considered for suspension, since commercial leverage matters but must support, never delay, the proportionate action needed to protect users.

Contractual escalation should run alongside regulatory obligations. Depending on the product and the organisation's role, notification to OPSS, a local authority, the MHRA, the Driver and Vehicle Standards Agency or another regulator may be required, and the UK Product Safety Database recorded 2,396 notifications covering 3,368 products in 2025/26, including 563 serious-risk and 259 high-risk cases. Procurement teams should know the relevant reporting route before an incident, not while searching for it afterwards.

Alternative supply becomes critical where quarantine, withdrawal or recall removes essential goods from service. The 2025/26 infant-formula incident is a useful public-sector example: the Food Standards Agency coordinated with the UK Health Security Agency, DHSC, the NHS, manufacturers and major retailers once affected products reached the UK, while officials assessed replacement availability. The wider international recall ultimately affected 99 countries, showing how response and continuity planning become inseparable in a genuine crisis.

Procurement should also protect the evidential record throughout. Purchase orders, specifications, supplier approvals, test reports, batch numbers, software versions, photographs and correspondence may later determine which products are affected and who bears the cost. Once immediate safety is controlled, commercial teams can enforce warranties, indemnities, replacement rights and recovery provisions, so the strongest response combines decisive user protection with disciplined contract management, ensuring urgency does not destroy the evidence required for subsequent accountability.

Building Product Safety into Category and Supply Chain Strategy

Product safety becomes strategic when it influences how a category is segmented, sourced and governed, rather than appearing as a late compliance checkpoint. Category strategies

should identify which products can cause serious harm, where critical components originate, how concentrated the supply base is and which suppliers possess credible technical capability, letting procurement direct stronger assurance to high-consequence categories while avoiding unnecessary bureaucracy for routine, low-risk purchases elsewhere in the portfolio.

Supply-market structure matters because safety and resilience can pull in different directions. Sole-source arrangements may preserve technical control but increase disruption exposure, while rapid multisourcing can introduce unfamiliar factories, components or quality systems. Category planning should therefore consider qualified alternatives before shortages occur, because dual sourcing is valuable only when both sources meet equivalent safety requirements; a second, unvalidated supplier may increase availability while simultaneously weakening the underlying product-safety case.

The financial scale justifies strategic treatment rather than ad hoc handling. OPSS estimated that 306,890 UK businesses fell within its regulatory scope in 2025, representing 11% of the business population and around £525 billion of combined turnover, excluding construction products, while OPSS also enforces construction-product requirements across markets estimated at roughly £109 billion. Product safety therefore touches a substantial part of the UK economy, not a narrow specialist corner.

Category managers should map safety dependencies as they would cost or geopolitical risk. A medical device may depend on sterilisation capacity, an e-bike on battery cells and chargers, a building product on fire-performance characteristics, and a connected appliance on ongoing software support; these dependencies should appear in sourcing plans, supplier segmentation, and contingency models. The objective is understanding which upstream failure could make an apparently ordinary purchased item unsafe or unavailable overnight.

Commercial incentives should reinforce safe behaviour, not undermine it. Contract structures that reward only unit-price reduction may encourage suppliers to find savings through materials, inspection frequency, or subcontracting. In contrast, balanced scorecards can recognise defect prevention, audit closure, change-control discipline, and traceability alongside cost and service. The strategic test is whether an organisation could quickly say which products could cause serious harm, where they came from, and how users would be reached if needed.

From Reactive Liability to Preventative Responsibility

Traditional product liability asks who should compensate after a defective product causes damage. Modern regulation increasingly asks an earlier question: who was best placed to identify and control the risk before harm occurred? The UK's 2026 product-safety consultation explicitly proposes proactive action across the supply chain, including clearer accountability and stronger obligations for online marketplaces, so liability remains important, but prevention is becoming an equally significant organising principle for product governance.

That shift is already visible in sector-specific law rather than remaining aspirational. Since June 2025, Great Britain's medical-device post-market surveillance regime has required manufacturers to gather and analyse safety and performance information after products enter use, investigate serious incidents and take preventive or corrective action where necessary, treating market placement as the beginning of a monitoring obligation rather than the end of regulatory scrutiny, particularly where risk only becomes visible through real-world use.

The Product Regulation and Metrology Act 2025 provides powers to modernise further the framework, including regulation of online marketplaces, software, and other intangible components. However, the Act does not itself impose every future duty, since secondary legislation is required. Preventative responsibility also changes procurement behaviour: buyers should not rely on the prospect of damages after failure where loss involves injury or reputational harm that money cannot reverse.

Private-sector assurance shows the same preventative direction developing voluntarily alongside regulation. The British Toy and Hobby Association's Lion Mark identifies members committed to its Code of Practice, with licence holders subject to periodic systems appraisal. At the same time, BSI Kitemark certification provides independent testing and continuing surveillance across a range of products. Neither replaces statutory compliance, but both illustrate how credible suppliers can build verification and preventative assurance beyond the minimum act of declaring that a product complies with the law.

Data as a Product Safety Tool

Product-safety data turns isolated complaints into patterns. Useful sources include warranty claims, customer contacts, incident reports, repair records, returns, test results, connected-product telemetry and regulatory databases. Individually, one overheating charger or broken component may look incidental; aggregated across thousands of units, the same signal may reveal a defect requiring intervention, so the challenge is not merely collecting information but linking it to product identity, batch, configuration, supplier and date of manufacture.

The UK Product Safety Database demonstrates the value of structured intelligence from many contributors, not just one. In 2025/26, it received 2,396 notifications covering 3,368 products, of which 563 were classified as serious risk and 259 as high risk; among notifications with recorded harm types, fire accounted for 424 and electric shock for 226. OPSS cautions that these figures support risk prioritisation but do not measure national prevalence.

Connected products can provide even richer evidence because performance can be observed continuously rather than inferred from returned units. Temperature, battery health, error codes, failed logins, sensor anomalies and software faults may expose deterioration before injury occurs. Governance is essential around privacy, security and retention: data should support proportionate safety decisions, not create unfiltered surveillance, and the strongest systems connect telemetry with engineering thresholds and human investigation rather than treat algorithmic alerts as conclusions.

AI for Product Safety – Both Risk and Solution

Artificial intelligence creates product-safety risk when its outputs influence physical behaviour, but the same technology can strengthen detection and surveillance. Machine-learning models can identify abnormal vibration, temperature, image patterns, failure combinations or complaint clusters faster than manual review across large datasets, with the greatest value arising where they support engineers and regulators by prioritising evidence for investigation, rather than becoming the sole authority for deciding whether a product is safe.

OPSS is already applying advanced analytics to enforcement rather than relying purely on manual targeting. Its 2025/26 Delivery Report describes a Border Inflow Modelling Tool using a Bayesian approach to UK import data to improve targeting of non-compliant consignments, a practical example of AI-related methods being used preventatively, so that limited inspection resources can be concentrated on higher-risk flows rather than spread evenly across low-risk trade at the border.

Healthcare provides another controlled environment for examining the same balance between risk and benefit. In April 2026, the MHRA received £3.6 million of Department of Health and Social Care funding over three years to expand its AI Airlock programme, the UK's regulatory sandbox for AI as a Medical Device. The programme examines technologies through supervised testing, post-market surveillance, validation and change-control exercises, generating evidence intended to inform future regulatory pathways and the safe deployment of AI medical technologies.

Procurement should apply the same dual perspective when buying AI-enabled safety tools. Buyers should evaluate training data, false positives, false negatives, drift, human escalation and evidence retention alongside accuracy claims, because a system that detects 99% of anomalies may still be unsuitable if the missing 1% contains catastrophic hazards. AI can

make assurance faster and more predictive, but accountable people must remain able to challenge outputs and stop unsafe products when evidence warrants intervention.

Global Products, Diverging Regulations

A product designed for global sale increasingly faces different legal regimes rather than one transferable compliance package. Great Britain, Northern Ireland and the EU provide the clearest example close to home: the General Product Safety Regulations 2005 continue to apply in Great Britain, while EU Regulation 2023/988 has applied in Northern Ireland since 13 December 2024 under the Windsor Framework, so one consumer product can face different traceability and marketplace requirements within the UK itself.

Conformity marking, liability, and AI rules are diverging along broadly similar lines within a few years of each other, driven by Brexit-era regulatory separation, new EU legislation, and the UK's domestic reform agenda under the Product Regulation and Metrology Act 2025. The table below summarises the current position for a product sold across Great Britain, Northern Ireland and the European Union, before any further changes are announced.

Aspect	Great Britain	Northern Ireland	European Union
General product safety regime	General Product Safety Regulations 2005	EU Regulation 2023/988 (since 13 Dec 2024, Windsor Framework)	Regulation (EU) 2023/988
Conformity marking	UKCA permitted; CE still recognised indefinitely for many categories	CE marking, or CE together with UKNI where a UK Approved Body undertakes mandatory third-party conformity assessment; UKNI is never used alone	CE marking
Product liability regime	Consumer Protection Act 1987 (no software-specific reform yet)	Consumer Protection (Northern Ireland) Order 1987 currently; Directive (EU) 2024/2853 is a replacement EU act and is due to apply to relevant Northern Ireland products from December 2026 under the Windsor Framework arrangements.	Directive (EU) 2024/2853, from 9 December 2026
AI as a safety component	Sector-led approach; powers under the Product Regulation and Metrology Act 2025	EU AI Act applies	Regulation (EU) 2024/1689 (EU AI Act)
Marketplace due-care duty	Proposed under the 2026 consultation; not yet in force	GPSR marketplace obligations apply	GPSR marketplace obligations (in force)

Great Britain continues to recognise CE marking indefinitely for many products covered by 21 regulations, while also permitting UKCA marking, though medical devices and construction products each follow separate transitional timetables. A multinational supplier therefore cannot safely assume that one declaration, certificate or label automatically satisfies every UK product category, even before considering requirements in the European Union, Northern Ireland, or further afield.

Liability is diverging as clearly as marking. The EU's Product Liability Directive 2024/2853 treats software as a product and applies to products placed on the market or put into service from 9 December 2026, expressly addressing software updates, cybersecurity-related safety and substantial modifications, including changes produced through continuous AI learning. Great Britain remains governed by the Consumer Protection Act 1987 unless Parliament

changes that framework, so cross-border claims increasingly risk different legal analyses on similar facts.

Regulatory divergence does not necessarily require different physical products, but it demands disciplined configuration management. Organisations should maintain jurisdiction matrices covering applicable legislation, standards, markings, responsible persons, language requirements, technical files, cybersecurity obligations and recall routes, and commercial teams must also control where goods may lawfully be sold, turning regulatory intelligence into an operational supply-chain capability rather than a periodic legal review conducted only when a problem arises.

Will Liability Follow the Product Throughout Its Digital Life?

Digital products challenge the assumption that liability should be fixed by an item's condition when first sold. A connected device may later receive software, security patches, cloud functions or AI changes controlled by its manufacturer long after purchase. The UK's 2026 consultation recognises that AI can adapt across a product's lifecycle and asks how regulation should respond, a question that points towards responsibility following whoever retains practical control over safety-relevant digital change after market placement.

The European Union is already moving explicitly in that direction. Directive 2024/2853 treats software as a product and defines manufacturer control to include software updates and upgrades supplied, authorised or enabled by the manufacturer, with recitals stating that manufacturers should remain liable for defectiveness arising after market placement where software or machine-learning algorithms remain within their control. The Directive applies to products placed on the market from 9 December 2026 onwards.

The same Directive also addresses substantial modification directly. A major software update, upgrade, or change produced by continuous AI learning can result in a product being treated as newly made available when the modification occurs. Where another economic operator substantially modifies a product outside the original manufacturer's control, that operator can itself be treated as the manufacturer for liability purposes going forward.

Great Britain has not yet adopted an equivalent replacement for the Consumer Protection Act 1987. The Product Regulation and Metrology Act 2025 supplies powers to regulate software and AI components for safety purposes, while the 2026 consultation explores lifecycle responsibility, but neither should be confused with a new civil product-liability regime already in force. Commercial contracts can anticipate that uncertainty by explicitly allocating responsibility for software maintenance, cybersecurity, model changes and end-of-support dates.

That position may itself change. The Law Commission is conducting a dedicated review of product liability in England and Wales, examining whether Part I of the Consumer Protection Act 1987 remains fit for purpose, particularly for digital products, software and emerging technologies including AI. Substantive work began in September 2025, and a formal public consultation on reform proposals is planned for the second half of 2026, placing continuing digital responsibility squarely within an active law-reform programme.

What Does Good Product Safety Governance Look Like?

Good product-safety governance starts with clear senior accountability. Boards and executive teams need not perform technical testing themselves, but should know which product categories can cause serious harm, who owns those risks and how incidents reach them. Governance should define decision rights for suspension, recall, regulatory notification and customer communication, since without that structure, organisations can lose critical time debating authority. Meanwhile, unsafe products remain in use or keep moving through the chain.

Technical competence must sit beneath governance rather than substitute for it. Product-safety decisions may require engineers, quality professionals, clinicians, cybersecurity

specialists or regulatory experts depending on the product, and procurement and legal teams cannot replace that expertise. However, they should ensure it is available and can independently challenge commercial pressure favouring continued supply. Senior committees should receive concise evidence on incidents and unresolved technical disagreements, not reassuring averages that conceal exceptional risk.

Metrics should show whether controls are actually working. Appropriate board-level indicators might include serious incidents, open recalls, overdue corrective actions, unauthorised changes, failed product tests, critical supplier audits and time taken to identify affected customers. Context matters more than volume: one unresolved fire hazard may deserve more attention than hundreds of minor defects, so good governance combines quantitative trend information with clear escalation thresholds and narrative explanations of high-consequence exceptions that require senior intervention.

Safety Cannot Be Outsourced.

Every organisation that helps place a product into a user's hands owns some element of the risk, even where another participant carries the primary statutory duty. This is a governance principle, not a statement of law: it does not mean every participant automatically incurs legal liability for a defect it neither caused nor could control. Manufacturers control design, importers provide a domestic route to market, distributors choose their supply, purchasers decide what evidence to accept.

Contracts can redistribute financial consequences, but responsibility for competent decisions cannot simply pass downstream and be forgotten, even where a court finds the statutory duty lay elsewhere. Outsourcing manufacturing does not outsource the consequences of selecting the manufacturer; using a marketplace does not remove the need to know the seller; buying a certified product does not remove the need to confirm the certificate matches what was delivered. Each intermediary adds distance, making visibility more important.

The digital era makes shared responsibility even more persistent. Software updates, cloud services, cybersecurity vulnerabilities, and adaptive AI can alter a product after purchase, so the organisation that can change safety-critical behaviour may remain involved for years. The EU's Product Liability Directive makes that logic explicit for software within manufacturer control. At the same time, the UK's 2026 consultation asks how regulation should address AI across its lifecycle, so product safety increasingly follows demonstrable control, not physical custody.

The commercial lesson is simple but demanding: no organisation should treat another participant's role as a substitute for its own competence. Suppliers must prove, purchasers must verify, marketplaces must increasingly police access, and regulators must intervene where market controls fail. Good supply chains distribute tasks without dispersing accountability; when responsibility is clear, evidence moves quickly, and unsafe products can be contained, but when everyone assumes somebody else owns the problem, risk reaches the user.

Summary – Designing Safety into the Supply Chain

Engineering alone does not create the safest product. It emerges from a supply chain in which requirements are clear, suppliers are competent, components are traceable, changes are controlled, and evidence is challenged rather than accepted. Engineering establishes the technical safety case, but procurement determines who is trusted to deliver it, and contract management tests whether that promise survives contact with reality across public and private markets alike.

That system must now extend beyond the traditional point of sale. Online marketplaces can connect UK consumers directly with overseas sellers; connected products can change through software; AI can adapt after deployment; cybersecurity failures, as WannaCry showed, can create real operational and clinical consequences. The concept of a finished product is

becoming less useful for many categories, and where safety-relevant behaviour evolves, monitoring, documentation and accountability must evolve with it.

Public and private markets differ in structure, but not in this underlying obligation. Public procurement operates within a proportionate statutory framework of conditions, KPIs and exclusion grounds; private purchasers rely more heavily on contract, insurance and reputation. Both nonetheless depend on the same four disciplines to convert good intentions into safe outcomes, and both have paid, in cases ranging from Grenfell and PPE Medpro to Takata and Cruise, for moments when one or more of those disciplines were missing.

A resilient supply chain is therefore built on four principles: accountability, visibility, verification and rapid intervention. Accountability identifies who must act; visibility reveals where products and components came from; verification tests whether claims are true; rapid intervention limits harm when controls fail. From Grenfell's construction products and Takata's airbags to PPE Medpro's gowns and Cruise's autonomous software, the recurring lesson is that serious consequences emerge when the gap between what is promised and what is independently verified becomes too wide.

When organisations embed accountability, visibility, verification and rapid intervention from specification through post-market monitoring, safety becomes part of commercial decision-making rather than a compliance afterthought bolted on at the end. The objective is not to eliminate every failure, since no supply chain can guarantee perfection across millions of transactions, but to reduce the probability and severity of harm, and to respond quickly and honestly when risk nonetheless emerges into the open.

Additional articles can be found at [Procurement and Supply Chain Management Made Simple](#). This site looks at procurement and supply chain management issues to assist organisations and people in increasing the quality, efficiency, and effectiveness of their product and service supply to the customers' delight. © Procurement and Supply Chain Management Made Simple. All rights reserved.

Sources and Further Reading

Legislation and official guidance

- *Product Regulation and Metrology Act 2025* ([legislation.gov.uk](#))
- *Procurement Act 2023 and Cabinet Office statutory and Procurement Policy Notes guidance, including PPN 009 on modern slavery* ([gov.uk](#))
- *Consumer Protection Act 1987; Consumer Rights Act 2015; Unfair Contract Terms Act 1977; Sale of Goods Act 1979*
- *Law Commission – Product Liability project and Terms of Reference*
- *Product Security and Telecommunications Infrastructure Act 2022 and the PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023*
- *Automated Vehicles Act 2024; Automated and Electric Vehicles Act 2018*
- *Department for Business and Trade, Product Safety Review consultation, March 2026* ([gov.uk](#))
- *Grenfell Tower Inquiry, Phase 2 Report (September 2024) and the Government Response to the Grenfell Tower Inquiry Phase 2 Report (February 2025)* ([gov.uk](#))

Regulators and enforcement bodies

- *Office for Product Safety and Standards, Annual/Delivery Report 2025/26, UK Product Safety Database, and Product Recalls and Alerts service* ([gov.uk/opss](#))
- *Medicines and Healthcare products Regulatory Agency, AI Airlock programme reports and Field Safety Notice database*

- *National Cyber Security Centre, guidance on the security of operational technology and connected devices*
- *Vehicle Certification Agency and Driver and Vehicle Standards Agency, software-update and type-approval guidance*
- *Intellectual Property Office, counterfeiting and piracy research and enforcement statistics*

EU and international sources

- *Regulation (EU) 2023/988 on general product safety*
- *Directive (EU) 2024/2853 on liability for defective products*
- *Regulation (EU) 2024/1689, the EU Artificial Intelligence Act*
- *US National Highway Traffic Safety Administration, consent order and penalty notices concerning Cruise LLC (2024)*

Standards, insurance and industry bodies

- *BSI, PAS 7100:2022, Product recall and other corrective actions – Code of practice*
- *Association of British Insurers, guidance on product liability insurance*
- *Lloyd's Market Association, Product Recall Committee market commentary*
- *Which?, product safety investigations and marketplace testing reports*

Selected incidents and recalls

- *National Audit Office investigation into WannaCry and the NHS*
- *NHTSA/US Department of Justice material concerning Cruise*
- *NHTSA material on Takata airbag recalls*
- *US Consumer Product Safety Commission material on the Samsung Galaxy Note7 recall*
- *OPSS material concerning the Haier tumble-dryer corrective programme.*

Case law and practitioner texts

- *Secretary of State for Health and Social Care v PPE Medpro Limited [2025] EWHC 2486 (Comm), judgment of Mrs Justice Cockerill DBE, 1 October 2025*
- *Clerk & Lindsell on Torts (Sweet & Maxwell)*
- *Chitty on Contracts (Sweet & Maxwell)*
- *Benjamin's Sale of Goods (Sweet & Maxwell)*