

***When Products Fail –
Safety, Liability and Accountability
Across the Supply Chain***



Procurement and Supply Chain Management Made Simple.

Index

<i>Section</i>	<i>Page</i>
<i>Foreword</i>	<i>4</i>
<i>Introduction — Unsafe by Design</i>	<i>5</i>
<i>What Makes a Product Unsafe?</i>	<i>5</i>
<i>From Factory to Consumer — The Product Safety Chain</i>	<i>6</i>
<i>One Product, Many Potentially Responsible Parties</i>	<i>7</i>
<i>The UK Product Safety Framework</i>	<i>7</i>
<i>The Consumer Protection Act 1987 — Strict Product Liability</i>	<i>8</i>
<i>Negligence — When Reasonable Care Is Not Enough</i>	<i>8</i>
<i>Contractual Liability for Unsafe Products</i>	<i>9</i>
<i>Regulatory Liability Versus Civil Liability</i>	<i>10</i>
<i>Proving That a Product Was Defective</i>	<i>10</i>
<i>Defences, Causation and Contributory Factors</i>	<i>11</i>
<i>Time Limits and Long-Tail Product Liability</i>	<i>11</i>
<i>The Product Regulation and Metrology Act 2025</i>	<i>12</i>
<i>Why the Existing Product Safety Framework Is Being Rebuilt</i>	<i>13</i>
<i>The UK's New Product Safety Framework — The 2026 Proposals</i>	<i>13</i>
<i>Accountability Throughout the Supply Chain</i>	<i>14</i>
<i>Market Surveillance and the Future of Enforcement</i>	<i>14</i>
<i>Great Britain, Northern Ireland and the European Dimension</i>	<i>15</i>
<i>The Manufacturer — Where Responsibility Begins</i>	<i>16</i>
<i>Component Suppliers — When the Defect Starts Further Upstream</i>	<i>16</i>
<i>The Importer — More Than a Logistics Function</i>	<i>17</i>
<i>The Distributor — The Duty Not to Look the Other Way</i>	<i>17</i>
<i>The Retailer — The Final Gatekeeper</i>	<i>18</i>
<i>Own-Brand Products and Private Labels</i>	<i>19</i>
<i>Overseas Manufacturers and Complex Global Supply Chains</i>	<i>19</i>
<i>Fulfilment Providers, Warehouses and Logistics Operators</i>	<i>20</i>

<i>Section</i>	<i>Page</i>
<i>Conformity Assessment and Product Certification</i>	<i>20</i>
<i>UKCA, CE Marking and Recognised Standards</i>	<i>21</i>
<i>Testing, Certification and Third-Party Assurance</i>	<i>22</i>
<i>When the Certificate Is Wrong</i>	<i>22</i>
<i>Supplier Assurance — Trust but Verify</i>	<i>23</i>
<i>Traceability — Knowing Where the Product Came From</i>	<i>23</i>
<i>Traceability Beyond Tier One</i>	<i>24</i>
<i>Technical Files and the Product Safety Audit Trail</i>	<i>24</i>
<i>Digital Product Information and the Future of Traceability</i>	<i>25</i>
<i>When Records Are Missing</i>	<i>26</i>
<i>The First Safety Incident</i>	<i>26</i>
<i>Product Safety Risk Assessment</i>	<i>27</i>
<i>Corrective Action — Repair, Warning, Withdrawal or Recall?</i>	<i>27</i>
<i>Product Recalls — Who Pays?</i>	<i>28</i>
<i>Notification to Regulators</i>	<i>28</i>
<i>Crisis Management and Consumer Communication</i>	<i>29</i>
<i>The Cost of Acting Too Late</i>	<i>30</i>
<i>Summary — Safety Is a Supply Chain Responsibility</i>	<i>30</i>
<i>Sources and Further Reading</i>	<i>31</i>
<i>Legislation</i>	<i>31</i>
<i>Case Law</i>	<i>32</i>
<i>Official Reports, Regulatory Guidance and Consultations</i>	<i>32</i>
<i>Further Reading</i>	<i>32</i>

Foreword

A defective product rarely begins with a single bad decision. Before reaching a customer, it may pass through designers, component suppliers, manufacturers, testing laboratories, importers, distributors, warehouses, retailers and online marketplaces. Each participant makes decisions about specification, materials, testing, certification, storage, labelling, traceability and sale. Product safety is therefore the accumulated result of a supply chain's choices, controls and omissions, spread across many hands, rather than the responsibility of one factory acting alone.

Commercial distance does not eliminate responsibility. Government guidance makes it clear that organisations that manufacture, import, distribute, or sell consumer products in the UK all carry product-safety responsibilities. Manufacturers and importers must demonstrate compliance and support traceability, while sellers must not supply products they know, or should have known, are unsafe. Once products reach the market, monitoring complaints, incidents, and emerging risks becomes part of responsible supply chain management rather than an optional quality exercise.

The central question is therefore not simply who manufactured the defective item, but who had the opportunity to prevent, detect or control the risk. A purchaser may specify the product; a component supplier may introduce the defect; an importer may admit it to the market; a retailer may receive the first complaints. When products fail, liability may follow several paths simultaneously, making product safety a shared commercial, regulatory and legal responsibility across the supply chain.

Introduction — Unsafe by Design

Product safety is no longer a question confined to engineers inspecting a finished item before it leaves a factory. Modern products are assembled through international networks of designers, component manufacturers, importers, logistics providers and retailers, each capable of creating or amplifying risk. OPSS, now part of the Department for Business, Innovation, Science and Trade after the July 2026 departmental merger, estimated that businesses within its regulatory scope generated about £525 billion of turnover in 2025.

The risk is equally visible in enforcement data. During 2025-26, the UK Product Safety Database received 2,396 notifications covering 3,368 products. Of those notifications, 563 were recorded as serious risk and 259 as high risk. Fire accounted for 424 reported harm classifications, electric shock for 226 and injuries for 194. These figures are not estimates of national prevalence, but they demonstrate the breadth and persistence of unsafe or non-compliant products still reaching the market.

A product may be legally compliant when first supplied yet become hazardous through deterioration, improper maintenance, modification, counterfeit replacement parts or software changes. Conversely, an apparently well-made item may have been unsafe from the outset because a foreseeable use was overlooked, a warning was inadequate or a component failed under realistic conditions. Safety, therefore, involves design, sourcing, manufacture, conformity assessment, distribution, information, traceability, and post-market monitoring, rather than a single quality-control checkpoint.

Whirlpool's tumble-dryer programme remains the clearest illustration of how a technical defect becomes a supply-chain and governance problem. Parliamentary evidence recorded 5.3 million affected machines manufactured for the UK market and at least 750 fires linked to the lint-related fault. In 2019, OPSS informed Whirlpool that it intended to serve a Recall Notice, after which the company recalled unmodified machines already in homes. Product safety is consequently a lifecycle obligation, not simply a factory-gate test.

What Makes a Product Unsafe?

Unsafe products arise through different failure mechanisms, and the distinction matters because it influences evidence, accountability and corrective action. A design defect may affect every unit produced; a manufacturing defect may concern one batch. Component failures can originate several tiers upstream, while contamination may occur during production, packaging, storage or transport. Investigation therefore begins by asking not merely what failed, but when, where and through whose process the hazard entered the product.

Design safety requires consideration of foreseeable behaviour, not merely ideal use. The General Product Safety Regulations 2005 require consumer products in Great Britain to be safe under normal or reasonably foreseeable conditions of use. That reaches beyond compliance with instructions: children may access battery compartments, users may overheat appliances, furniture may be climbed upon, and equipment may be assembled imperfectly. A warning cannot automatically cure a design that exposes users to an avoidable, foreseeable hazard.

CASE STUDY

Manufacturing variation creates a different problem, because materials may be substituted, tolerances may drift, welds may weaken, or sterilisation may fail despite an adequate original design. The 2025 High Court dispute involving PPE supplier Medpro is an unusually clear public-sector example: the Department of Health and Social Care had paid £121,999,219.20 for surgical gowns, and the court found breaches concerning validated sterility, EN 556-1 compliance and CE marking.

The court in that case awarded the full contract value as damages, but it also rejected DHSC's separate £8,648,691 storage-cost claim because the supporting evidence was inadequate. The judgment shows why certification and paperwork cannot be separated from physical performance: the gowns were intended as sterile medical devices, yet testing and evidential analysis became central to determining whether the contracted product had actually been supplied. Safety failures can therefore generate two distinct battles.

Warnings and instructions form part of safety because users cannot manage risks they have not been told about. The issue is especially acute where hazards are hidden, cumulative or counter-intuitive. In 2025-26, choking accounted for 142 Product Safety Database harm classifications and chemical risks for 145. A child-resistant enclosure, clear age restriction or adequate hazard warning may therefore be as safety-critical as the material from which a product is actually made.

Digital functionality further destabilises the idea of a finished product. Connected devices can acquire new features after sale, while software faults may alter charging, temperature control, braking, sensing or automated decision-making. The Product Security and Telecommunications Infrastructure Act 2022 already imposes continuing compliance duties on manufacturers, importers and distributors of relevant connectable products. Product safety increasingly has to accommodate physical components whose real-world behaviour is partly governed by code that can change after purchase.

From Factory to Consumer — The Product Safety Chain

Product safety responsibilities begin with the manufacturer, which normally controls design, production and initial conformity assessment. Yet the finished product may incorporate batteries, electronic boards, chemicals, fasteners, packaging and software supplied by others, and each input can introduce a latent defect. Effective control, therefore, depends on approved specifications, supplier qualification, incoming inspection, change management, and traceability, so a manufacturer cannot safely treat component purchasing as a purely commercial exercise divorced from engineering risk.

Importers occupy an important position because they introduce products from outside the relevant market into the domestic supply chain. Government guidance stresses that businesses bringing goods into Great Britain from the EU may now be importers rather than distributors, carrying additional compliance responsibilities they may not have anticipated. Import status can therefore change legal exposure without changing the physical activity of buying and reselling, so procurement teams need to understand where legal responsibility attaches.

Distributors and retailers are not passive conduits. Under the General Product Safety Regulations 2005, distributors must act with due care, avoid supplying products they know or should presume to be dangerous, retain traceability documentation, and cooperate with producers and enforcement authorities. OPSS guidance likewise states that businesses selling consumer products must not sell products they know, or should have known, are unsafe. Commercial distance from the factory does not create regulatory distance from the hazard.

Fulfilment providers, warehouses and online marketplaces further complicate the chain because physical possession, contractual sale and digital presentation can reside with different organisations. In 2025-26, the removal of an online listing was recorded 594 times as a corrective action in the Product Safety Database, while 1,102 corrective actions involved the rejection of imports at the border. Product-safety interventions increasingly occur before, during and after conventional retail distribution rather than only at the point of manufacture.

The modern chain therefore operates as a sequence of safety gates rather than a simple manufacturer-to-retailer pipeline. Designers control foreseeable hazards; component suppliers control inputs; manufacturers integrate them; importers verify market entry; distributors preserve compliance; retailers face consumers; and marketplaces influence

access to buyers. When any one gate fails, the next economic actor may still possess information, control or legal duties capable of preventing harm before the product ever reaches its user.

One Product, Many Potentially Responsible Parties

A single incident can engage several forms of responsibility at once. The manufacturer may face strict product-liability exposure; an importer may have regulatory duties; a retailer may owe contractual rights to the purchaser; and another participant may be liable in negligence. Those routes are not mutually exclusive, so the injured person, enforcement authority, insurer, purchaser and organisations within the supply chain may each pursue different remedies arising from the same defect.

The Consumer Protection Act 1987 illustrates that breadth in Great Britain. Liability can attach to the producer, an own-brand holder that holds itself out as producer, and qualifying importers; a supplier can become liable in specified circumstances if it fails to identify the relevant producer or supplier after a proper request. Northern Ireland has parallel provisions under the Consumer Protection (Northern Ireland) Order 1987, so identifying the contracting seller alone can miss legally significant parties.

Hastings v Finsbury Orthopaedics Ltd and Stryker UK Ltd demonstrates how componentised products complicate attribution. The claimant's metal-on-metal hip replacement combined components manufactured by separate respondents, and the Supreme Court considered whether the resulting prosthesis was defective under the 1987 Act. The claim ultimately failed on defect, but the litigation shows how complex assemblies can simultaneously place component design, system interaction, clinical evidence, and producer responsibility before the court.

Commercial contracts then redistribute the financial consequences behind statutory liability. A retailer may compensate a consumer and seek recovery from its supplier; an importer may rely on warranties from an overseas manufacturer; insurers may exercise subrogation rights; and contribution claims may arise between defendants. Contractual indemnities can allocate costs between organisations, but they do not eliminate statutory duties to consumers or regulators, so product safety creates a network of liabilities rather than a single upstream line.

The UK Product Safety Framework

A single code does not govern UK product safety. In Great Britain, the General Product Safety Regulations 2005 set a baseline for consumer products, requiring them to be safe in normal or reasonably foreseeable use, while product-specific legislation applies where relevant. OPSS lists regimes covering areas such as toys, electrical equipment, machinery, gas appliances, cosmetics, fireworks, and personal protective equipment, resulting in an overlapping architecture in which a product's classification determines the applicable duties.

Northern Ireland now follows a different general regime. Since 13 December 2024, Regulation (EU) 2023/988 on general product safety has applied there, replacing the 2005 Regulations for general product safety. Sector-specific EU rules also continue to operate where applicable under the Windsor Framework. A product sold throughout the United Kingdom may therefore face different regulatory routes in Great Britain and Northern Ireland, even though commercial teams may treat the UK as one sales territory.

Responsibility is also divided institutionally. OPSS, part of the Department for Business, Innovation, Science and Trade since the July 2026 merger, remains the national regulator for most consumer goods and construction products, while local Trading Standards authorities retain market-surveillance functions. The Food Standards Agency regulates food; the MHRA regulates medicines and medical devices; the DVSA oversees vehicle safety; and the Health and Safety Executive regulates workplace products.

That regulatory footprint is easier to grasp in scale. OPSS estimated 306,890 businesses were within its regulatory scope in 2025, representing about 11% of the UK business population

and generating the £525 billion combined turnover already noted, while construction products, also enforced by OPSS, represented a further £109 billion market. Product regulation is consequently not a specialist concern at the margins of commerce: it governs supply chains carrying hundreds of billions of pounds.

Enforcement is correspondingly varied. Authorities can investigate, inspect goods, obtain technical documents and use measures including suspension, withdrawal, recall and prosecution, depending on the governing legislation. The 2025-26 Product Safety Database recorded at least one corrective action for 2,072 of 3,368 notified products, with recorded actions including 611 destructions, 479 recalls from end users and 429 seizures. These figures show that non-compliance can lead directly to stock loss, operational disruption and customer remediation.

The framework is also in transition. The Product Regulation and Metrology Act 2025 created broad powers for modernised secondary legislation, while Government consultations published in March 2026 proposed a new core product-safety framework and consolidated market-surveillance approach. Those proposals were still proposals in September 2026, not a wholesale replacement already in force. Organisations must therefore comply with current legislation while preparing for a regulatory model built around clearer supply-chain accountability and modern products.

The Consumer Protection Act 1987 — Strict Product Liability

Part I of the Consumer Protection Act 1987 establishes the principal statutory product-liability regime for Great Britain. It imposes strict liability: the claimant need not prove the producer's negligence, but must still establish a defect, damage and causation. Northern Ireland uses the parallel Consumer Protection (Northern Ireland) Order 1987; the new EU Product Liability Directive will apply to relevant Northern Ireland products placed on the market or put into service after 9 December 2026.

Under the 1987 Act, a product is defective when its safety is not such as persons generally are entitled to expect, taking all the circumstances into account. That is not the same as asking whether the product could have been safer or whether an adverse event occurred. The courts assess the safety expected from the product in context, including its presentation, reasonably expected use and the time at which it was supplied to the market.

Liability can extend well beyond the physical manufacturer. The Act covers producers, organisations presenting themselves as producers through their name or trade mark, and qualifying importers; suppliers may also face liability if, after a proper request, they fail to identify an appropriate producer or upstream supplier within a reasonable period. That structure matters most for private-label sourcing, where the commercial brand visible to the customer may differ entirely from the factory that manufactured the goods.

Recoverable damage under the statutory regime includes death and personal injury, together with qualifying damage to property intended for private use or consumption. A £275 threshold applies to property damage, and the defective product itself is not treated as compensable property damage. The regime is therefore not a general warranty scheme: it compensates specified harm caused by defective products, while purely commercial loss is usually pursued through contract, negligence or other legal routes instead.

The Supreme Court's 2022 decision in *Hastings v Finsbury Orthopaedics and Stryker UK* underlines the point. Mr Hastings alleged that a metal-on-metal hip prosthesis was defective, but the courts rejected the claim because statistical evidence did not establish a defect, and inherent risk did not automatically make it defective. Strict liability removes the need to prove fault; it does not remove the claimant's burden of proving that the statutory safety standard was not met.

Negligence — When Reasonable Care Is Not Enough

Negligence remains important where the facts concern careless design, manufacture, testing,

warning or distribution. Unlike statutory strict liability, negligence requires proof of fault: a duty of care, breach of that duty, causation and legally recoverable damage. The claimant must show that the defendant failed to exercise the standard of reasonable care expected in the circumstances. Good intentions, internal procedures and regulatory certificates may all be evidence, but none automatically proves reasonable care.

The foundation remains *Donoghue v Stevenson*, decided by the House of Lords in 1932 after Mrs Donoghue alleged illness from ginger beer containing a decomposed snail. The manufacturer had no contract with her, yet the case established that a manufacturer could owe a duty to the ultimate consumer. Nearly a century later, the principle still matters whenever an injured person needs to look beyond the immediate seller to the organisation whose conduct created the danger.

Reasonable care is dynamic because the precautions expected depend on foreseeable risk, technical knowledge and the seriousness of potential harm. A supplier of decorative goods may require different controls from a manufacturer of medical devices, lifting equipment or children's products. As knowledge evolves, continued reliance on an outdated test report or a historical design assumption may become unreasonable, so post-market complaints, near misses and regulator alerts can affect what a responsible organisation should investigate.

Negligence can coexist with contractual and statutory claims arising from the same facts. A defective component may trigger a consumer claim against a retailer, strict liability against a producer and negligence allegations against a designer or manufacturer. The claimant must prove that the breach caused the loss, while defendants may dispute alternative causes, misuse or later modification. Product-safety records should therefore demonstrate the compliance, reasoning and testing decisions that show reasonable care throughout the lifecycle.

Contractual Liability for Unsafe Products

Contract law operates alongside product-safety regulation by asking whether the seller supplied what was actually promised. In consumer sales, the Consumer Rights Act 2015 requires goods to be of satisfactory quality, fit for purpose and as described; safety is expressly an aspect of satisfactory quality. Consumers normally have a 30-day short-term right to reject non-conforming goods. These rights focus on the trader-consumer relationship, even where the underlying defect originated much further upstream.

Business-to-business sales are commonly governed by the Sale of Goods Act 1979 together with the parties' own negotiated terms. Implied obligations concerning satisfactory quality and fitness may apply, but commercial contracts often include detailed specifications, inspection rights, warranties, acceptance procedures and remedies. For public authorities and large private purchasers, those express provisions can be decisive because they define the exact performance purchased and the evidence required when goods fail testing, certification or operational use.

The PPE Medpro litigation shows the financial significance of precise drafting. DHSC paid £121,999,219.20 for 25 million surgical gowns at £4.88 each. The High Court found breaches concerning a validated sterility process, EN 556-1 and CE marking. Although DHSC had not effectively rejected the gowns within the contractual machinery, it recovered the full contract value as damages because the goods could not perform the sterile-gown function for which they had been purchased.

The same judgment also demonstrates that winning on breach does not guarantee recovery of every claimed cost. DHSC sought £8,648,691 for storage between February 2021 and June 2024, but the court rejected that element on the ground that the evidential foundation was inadequate. Contract management therefore matters after a safety failure as much as before: storage invoices, disposal records, testing costs, replacement purchases, and mitigation decisions may all need to withstand detailed scrutiny years later.

Specifications should translate safety expectations into measurable contractual obligations. References to legislation and standards are useful, but purchasers may also need defined materials, prohibited substitutions, approved factories, testing protocols, sampling levels, certificates, traceability fields and notification duties. A broad promise to supply “compliant” goods can leave avoidable arguments about what compliance actually requires. Strong procurement documents connect the technical specification, quality plan, acceptance criteria and remedies so safety requirements remain enforceable throughout performance.

Contractual remedies also sit behind consumer-facing obligations. A retailer that refunds customers may seek reimbursement from its distributor; an importer may claim against an overseas manufacturer; and a public authority may pursue damages where supplied goods cannot safely perform their intended function. Indemnities, insurance requirements and liability caps influence where the financial burden ultimately rests. However, none permits a party to contract out of regulatory obligations or eliminate rights that legislation makes non-excludable.

Regulatory Liability Versus Civil Liability

Regulatory enforcement and civil liability answer different questions. A regulator asks whether legal safety requirements have been breached and what intervention is needed to protect the market; an injured person or purchaser asks whether compensation or another private remedy is available. The same facts can support both processes, but neither automatically determines the other: a recall may occur without personal-injury litigation, while a claimant may recover damages even though no regulator has prosecuted anyone.

Regulatory tools are designed primarily to stop risk. Depending on the legislation, authorities may suspend supply, prohibit placing a product on the market, require warnings, order withdrawal or recall, seize goods and prosecute offences. During 2025-26, the Product Safety Database recorded 3,986 corrective actions, including 1,102 border rejections, 611 destructions, 594 online listing removals and 479 recalls from end users, so one unsafe product can trigger intervention at several points at once.

Criminal enforcement can add direct financial and reputational consequences. In March 2024, Diva Gift Limited was sentenced after pleading guilty to supplying a toy that failed essential safety requirements. Northampton Magistrates’ Court imposed a £10,000 fine, £4,393.16 costs and a £2,000 victim surcharge, totalling £16,393.16. The figures are modest compared with a major recall, yet the case shows that documentary or design failures can move into formal prosecution.

Civil claims focus instead on loss suffered by particular claimants. Depending on the facts, compensation may be pursued through strict product liability, negligence, contract or specialist statutory causes of action, and the measure of loss may include personal injury, property damage, replacement costs or contractual losses, subject to the rules governing each cause of action. Insurance may fund defence or settlement, but regulatory compliance and civil exposure remain legally distinct and must be managed separately.

Organisations therefore need two response tracks after a serious incident. The safety team must assess risk, notifications, containment and corrective action; the legal and commercial teams must preserve evidence and analyse claims, contracts, insurance and potential recovery against suppliers. Communications must support both tracks without delaying urgent protection of users. Treating a recall solely as litigation can endanger consumers, while treating it solely as an operational problem can destroy evidence needed to defend substantial losses.

Proving That a Product Was Defective

Product-liability disputes turn on evidence. The claimant must identify the product, establish the alleged defect, prove legally recognised damage and connect that damage causally to the defect. Serial numbers, batch codes, purchase records, photographs, retained samples and incident reports may determine whether the correct product can even be examined. Where

the item has been destroyed, repaired or altered, contemporaneous evidence matters because later testing may no longer reproduce its original condition.

Technical evidence requires more than showing that an accident occurred. Engineers may examine design tolerances, fracture surfaces, electrical protection, thermal behaviour or foreseeable loading; laboratories may test composition, contamination or sterility; clinicians may analyse biological causation. In A v National Blood Authority, claims concerning hepatitis C-infected blood required the High Court to assess defect by reference to the safety persons were entitled to expect, keeping scientific evidence and the legal test carefully distinct.

The metal-on-metal hip litigation provides another warning against treating adverse outcomes as proof of defect. In Gee v DePuy International, six lead claims were selected from group litigation concerning Pinnacle hip prostheses, and extensive expert evidence addressed metal wear, revision rates and biological response. The court emphasised that the statutory inquiry concerns the product's objectively assessed safety, not simply whether it contained a flaw or a claimant was injured after receiving it.

Defences, Causation and Contributory Factors

Strict product liability is not absolute liability. Section 4 of the Consumer Protection Act 1987 gives defendants specific statutory defences, including that the defect resulted from compliance with a legal requirement, the defendant never supplied the product, the defect did not exist at the relevant time, or the state of scientific and technical knowledge was insufficient to discover it. The defendant bears the burden of establishing whichever defence it relies upon.

The development-risks defence is deliberately narrow. It concerns the state of scientific and technical knowledge at the time the product was supplied, rather than whether an individual manufacturer actually knew of the danger. In A v National Blood Authority, involving 114 claimants infected with hepatitis C through blood or blood products, the High Court held that a known but then unavoidable risk was not transformed into an undiscoverable development risk merely because screening was unavailable.

Abouzaid v Mothercare illustrates the distinction particularly well. A child suffered severe eye damage when an elasticated strap and metal buckle recoiled while a pushchair accessory was being fitted. Mothercare argued that the hazard had not previously been recognised, but the Court of Appeal rejected the development-risks defence: the defect could have been identified through a simple practical test, and no scientific or technological advance was needed for the risk to become discoverable.

Causation remains a separate hurdle. A claimant must establish that the defect caused the relevant damage, not simply that a product failed before an injury occurred. Subsequent repair, abnormal loading, poor maintenance, misuse, counterfeit replacement parts or unauthorised software modification may provide alternative explanations. An intervening act can sometimes break the causal chain; in other cases it merely contributes to the outcome, leaving responsibility divided among several actors rather than eliminated.

Foreseeable misuse is different from extraordinary misuse. Product safety is assessed against use that can reasonably be expected, so a producer cannot necessarily escape liability because a consumer behaved imperfectly. Where the claimant's own fault contributes to the damage, section 6 of the 1987 Act applies contributory-negligence principles, permitting damages to be reduced. For component producers, a separate defence exists where the defect is wholly attributable to the subsequent product's design or instructions.

Time Limits and Long-Tail Product Liability

Product liability can linger long after the purchasing decision has faded from operational memory. In England and Wales, claims under Part I of the Consumer Protection Act 1987 are generally subject to three years running from the later of accrual and the claimant's relevant date of knowledge. Overlaying that is an absolute ten-year long-stop from the statutory "relevant time", which can extinguish the right even before damage or knowledge emerges at

all.

Other causes of action run on entirely different clocks. A simple contractual claim in England and Wales ordinarily has a six-year limitation period from the accrual of the claim. In contrast, an action on a speciality, including many deeds, generally has a twelve-year limitation period. Negligence claims involving latent non-personal-injury damage may engage a three-year knowledge-based period and a fifteen-year overriding long-stop. Scotland and Northern Ireland have distinct limitation and prescription regimes of their own.

The commercial consequences last still longer. Manufacturers are commonly required by product legislation to retain technical documentation for about ten years. However, sector rules vary because claims, recalls and regulatory investigations may surface long after production stops. *Hastings v Finsbury Orthopaedics* reached the Supreme Court in 2022 after a hip prosthesis implanted in 2009 was revised in 2012, showing how supplier exits, acquisitions and lost records can rival the original engineering evidence in importance.

The Product Regulation and Metrology Act 2025

The Product Regulation and Metrology Act 2025 received Royal Assent on 21 July 2025, with most of its provisions coming into force that day; sections 11(1) and 11(3) were expressly left to be brought into force by later commencement regulations. Its significance lies less in creating a new safety code than in giving ministers a broad statutory platform for modernisation. The Secretary of State may make product regulations to reduce or mitigate risks, ensure products operate effectively and regulate measurement.

Those powers reach deeply into the product lifecycle. Regulations may address product characteristics, manufacture, installation, components, marketing, use, packaging, storage, transport, monitoring, testing, certification, record-keeping and the provision of safety information. Importantly, the statutory concept of components can encompass intangible elements such as software, enabling the legislative architecture to respond to connected and AI-enabled products rather than assuming that safety is fixed permanently at the point of manufacture.

Online commerce is equally prominent within the new powers. The Act allows product regulations to impose requirements on online marketplaces and other persons involved in making products available, addressing a gap that became increasingly visible as overseas sellers gained direct access to UK consumers. It also permits requirements concerning product monitoring, complaints, documentation, and information about risks, shifting product-safety accountability between digital intermediaries and conventional manufacturers, importers, and distributors.

Enforcement powers can also be reshaped through secondary legislation made under the Act. Regulations may provide for investigation, entry, search, inspection, seizure, production of documents, warnings, prohibition, withdrawal and recall. They may create or widen criminal offences and provide civil sanctions, including monetary penalties. Where an offence is created under the Act's powers, the maximum custodial penalty on indictment cannot exceed two years, allowing enforcement to become both more coherent and more flexible.

The delegated powers are substantial but not unrestricted. Regulations are made by statutory instrument; consultation is generally required; and stronger parliamentary scrutiny applies to specified uses, including powers of entry, the creation or widening of criminal offences, the amendment of primary legislation, the first use of powers concerning online marketplaces, and the first creation of a new category of regulated person. The Act also governs information sharing, cost recovery and devolved consent.

The Act has already moved beyond theory. The Noise Emission in the Environment by Equipment for Use Outdoors (Amendment and Transitional) Regulations 2025 were made under the powers conferred by it. They came into force on 13 April 2026, updating measurement methods and supporting continued recognition of relevant CE requirements in

Great Britain. That first use demonstrates the model: Parliament supplies broad powers, while product-specific technical obligations are amended progressively as standards, markets and technologies evolve.

Why the Existing Product Safety Framework Is Being Rebuilt

The case for reform begins with fragmentation. The Government identifies more than 150 pieces of product-safety and legal-metrology legislation across the landscape, with several sets of rules often applying to one product. General duties sit alongside sector regimes for machinery, electrical equipment, toys, cosmetics, pressure equipment, and many other categories, developed at different times, leaving regulators and businesses to navigate overlapping powers, terminology, and procedural requirements.

The core Great Britain consumer-safety regime also dates from a different commercial era. The General Product Safety Regulations 2005 remain the baseline for many consumer goods, yet online retail has transformed market access since their introduction. Government consultation data show online sales accounted for 25.4% of UK retail sales in March 2024, compared with 10.8% ten years earlier, so products can now reach households directly from sellers with no meaningful UK establishment.

Modern products compound that structural problem further still. A connected appliance may combine imported hardware, third-party firmware, cloud services and later software updates, while an AI-enabled product may change its behaviour over its lifecycle. Traditional legislation frequently assumes identifiable physical products moving through recognisable domestic supply chains. The Government's reform programme instead seeks rules capable of addressing new technologies, digital product information and international e-commerce without repeated bespoke statutory fixes.

Reform is therefore about effectiveness as much as it is about simplification. The March 2026 enforcement consultation said fragmented and overlapping powers can delay action, create confusion and encourage excessive reliance on criminal prosecution where a more proportionate civil response might suffice. Government proposals seek a common enforcement toolkit, clearer responsibilities and better information sharing. The ambition is not deregulation; it is to remove avoidable complexity while intervening faster on unsafe or non-compliant products.

The UK's New Product Safety Framework — The 2026 Proposals

On 31 March 2026, the Government published proposals for a new core product-safety framework alongside a companion consultation on market surveillance and enforcement. Both consultations closed on 23 June 2026. As at September 2026, the proposals should still be treated as proposals rather than existing replacement law. Their direction is nevertheless clear: a more coherent baseline that reflects modern products, routes to market, and supply chains, while retaining strong protection against unsafe goods.

A significant proposal is to broaden the core framework beyond consumer products. The consultation envisages coverage of "business products" supplied to organisations, including public bodies and charities for their own use, subject to exclusions such as food, medicines, medical devices, military equipment and certain specialist sectors. That matters for procurement because safety obligations would no longer turn so heavily on whether the immediate purchaser is a household, a local authority or a housing provider.

The Government proposes retaining a general requirement that products be safe, but modernising what the safety assessment must consider. Relevant factors would include product characteristics, interactions with other products, vulnerable users, reasonable consumer expectations, state of the art and products attractive to children. Cybersecurity risks arising from artificial intelligence or machine learning would also be explicitly included, recognising that software behaviour can create physical safety consequences without any conventional manufacturing defect.

Standards would remain important but not conclusive under the proposals. The consultation notes that around 3,500 designated standards currently support regulatory compliance in the UK. Following a designated standard can provide a presumption of conformity with specified legal requirements, yet compliance does not prevent a product from being found dangerous where evidence shows otherwise. Certification simplifies assurance, but it cannot substitute for risk assessment, monitoring or action when experience reveals an underestimated hazard.

Product information would also become more digital under the reforms. The Government proposes a “digital by default” approach under which some required information could be provided electronically, while essential physical identifiers and warnings would remain where necessary. This could reduce the need for repeated labelling and make compliance information easier to update. However, it raises governance questions about accessibility, persistence, and authenticity, particularly since Northern Ireland’s EU rules may still require information to be physically present on packaging.

The framework is intended to work prospectively rather than only after accidents occur. Producers would be expected to monitor products, investigate complaints and maintain records, while downstream actors would have clearer duties to respond to alerts and visible non-compliance. That reflects a regulatory philosophy: placing a safe product on the market is not the end of responsibility, and safety information from returns, incidents or software behaviour may create a continuing obligation to investigate and intervene.

Accountability Throughout the Supply Chain

The 2026 consultation proposes replacing assumptions about neatly separated economic actors with three functional categories: producers, onward suppliers and online marketplaces. The categories would not be mutually exclusive, recognising that one organisation can manufacture, import, brand, warehouse, sell and facilitate sales simultaneously. Accountability would follow from what an actor actually does and the information or influence it possesses, rather than from its preferred commercial description or contractual label.

For producers, the proposed duties go beyond initial conformity assessment. They would be prohibited from supplying unsafe products and, where reasonable and proportionate, expected to undertake sample testing, provide routes for complaints, investigate safety concerns and maintain records. Onward suppliers would have to exercise due care, understand relevant hazards, check alerts and recalls, perform appropriate physical checks where they possess products, and ensure storage or transport does not compromise safety.

The emerging principle is difficult to reconcile with “we relied on our supplier” as a complete governance answer. A purchaser may rely on upstream evidence, but verification should reflect product risk, warning signs and the actor’s ability to intervene. Repeated complaints, implausible certificates, unexplained substitutions or known recalls demand action. Supply-chain accountability is strongest when contractual rights, technical assurance, complaints intelligence and regulatory monitoring reinforce one another rather than sit in separate silos.

Market Surveillance and the Future of Enforcement

Market surveillance is the bridge between product rules on paper and products actually circulating through shops, warehouses, borders and websites. OPSS acts as the national product regulator for many goods, while local Trading Standards services retain substantial enforcement responsibilities and specialist regulators cover defined sectors. The difficulty is not merely identifying unsafe products; authorities must determine which legislation applies, who has jurisdiction and which intervention can lawfully stop further supply quickly.

The operational scale is considerable. OPSS reported resolving 14,019 enforcement cases during 2025-26, including 4,598 cases where businesses were signposted to guidance, 2,749 involving advice and 1,056 in which no non-compliance was identified. It also recorded 699 online listings removed, 41 improvement plans, 190 business undertakings and 21 enforcement actions, including prohibition, withdrawal and recall notices, ranging in practice

from informal guidance to compulsory market intervention.

Border activity exposes the volume of risk before goods reach consumers at all. During 2025-26, OPSS checked consignments containing more than 11.3 million goods and reported that over 2.7 million were unsafe or non-compliant, roughly one quarter of those examined. The regulator estimated avoided consumer detriment of about £81 million from unsafe goods and £209 million from non-compliant goods, and seized imported teeth-whitening products with a stated value exceeding £1 million.

The proposed enforcement framework would consolidate powers currently scattered across more than 150 legislative instruments into a common statutory toolkit. Authorities could draw on clearer powers for investigation, inspection, seizure, withdrawal, recall and other interventions without repeatedly navigating different procedural architectures. The Government also proposes mechanisms for information sharing among regulators, departments, emergency services and other specified bodies, since faster intelligence flow matters where one product appears simultaneously at ports, marketplaces and retailers.

Civil monetary penalties are another significant proposal within the reform package. The consultation considers fixed, variable and escalating penalties as alternatives to criminal prosecution, particularly where a proportionate financial sanction could secure compliance more efficiently. Importantly, it did not propose a headline percentage-of-turnover maximum or a specific universal GBP cap; seriousness, scale, impact and repeated or persistent breaches are among the factors contemplated, with criminal prosecution remaining available for the most serious conduct.

More flexible enforcement could change commercial risk calculations considerably. Product-safety failures already impose quarantine, testing, recall, storage, destruction and reputational costs before any penalty is imposed. A consolidated regime could enable faster formal intervention, while enforcement undertakings allow some breaches to be corrected without prosecution. For boards and procurement teams, the expected cost of weak compliance should include regulator intervention and operational disruption, not simply the probability of a criminal fine.

Great Britain, Northern Ireland and the European Dimension

Operating across the United Kingdom now requires businesses to distinguish regulatory geography as carefully as product category. In Great Britain, UK Conformity Assessed (UKCA) remains the domestic conformity marking for relevant regulated products, while CE marking continues to be recognised for many product types under the post-Brexit regime. Government guidance covers more than twenty product areas affected by UKCA and CE arrangements, so choosing a marking route depends on several variables at once.

Northern Ireland follows a different architecture under the Windsor Framework because relevant EU rules for manufactured products continue to apply there. Products that meet EU requirements can bear the CE marking. Where mandatory third-party conformity assessment is performed by a UK-based body for the Northern Ireland market, CE must generally be accompanied by UKNI; an EU-recognised notified body supports CE without UKNI, so UKNI functions as a market-access indicator rather than a substitute for conformity.

The divergence also extends to general product safety across the two jurisdictions. The EU General Product Safety Regulation has applied in Northern Ireland since 13 December 2024, while Great Britain continues to rely on the General Product Safety Regulations 2005 pending reform. Qualifying Northern Ireland goods can retain unfettered access to Great Britain, including goods carrying CE or CE plus UKNI where applicable, requiring a single distribution model supported by two distinct compliance analyses.

Further divergence is approaching in the law of civil liability itself. Directive (EU) 2024/2853 modernises European product liability rules, including the treatment of software, and is due to apply to relevant products placed on the Northern Ireland market or put into service there after

9 December 2026 once implemented. Great Britain continues to be governed by the Consumer Protection Act 1987 unless Parliament changes it, creating an important north-south distinction in liability exposure.

The Manufacturer — Where Responsibility Begins

Manufacturers sit at the centre of product safety because they normally determine design, materials, performance limits and production controls before downstream businesses see the goods. Great Britain guidance requires manufacturers to meet applicable design and manufacturing requirements, complete conformity procedures, prepare technical documentation and declarations where required, apply identification or conformity markings and cooperate with market-surveillance authorities. Outsourcing production does not necessarily remove manufacturer status where goods are marketed under another organisation's name.

Design control should begin with hazards rather than certificates. Risk assessment needs to consider intended use, foreseeable misuse, vulnerable users, component interactions and the consequences of a single-point failure. Testing must challenge those assumptions using appropriate standards, worst-case configurations and representative samples. In *Wilkes v DePuy International*, the C-Stem hip component had undergone fatigue testing beyond the applicable British Standard requirements; its subsequent fracture did not establish that the product was defective when supplied.

Production control is equally important because an approved prototype proves little if mass-produced units drift away from it. Material specifications, tolerances, calibration, supplier controls, inspection plans and change approval help ensure conformity across subsequent batches. Technical files should preserve the reasoning behind those controls, including design documents, risk assessments and test evidence. Government guidance indicates that records are commonly required to be retained for 10 years after each product enters the Great Britain market.

Post-market surveillance closes the loop between design assumptions and real-world evidence. Complaints, warranty returns, incidents, and near misses can reveal patterns that are unavailable during pre-market testing. Vauxhall's Zafira B experience demonstrates the governance consequences of delayed learning: a House of Commons Transport Committee investigation concluded that Vauxhall was too slow to initiate a full investigation into vehicle fires, and by February 2017, the company had reported 59 fires in vehicles that had already undergone their first recall.

The manufacturer's responsibility is both technical and organisational. Engineers need authority to stop production or investigate abnormal failure patterns; quality teams need reliable complaint data; procurement must control component changes; and leadership needs escalation routes when uncertainty justifies precautionary action. A conformity mark may support market access, but it does not freeze the safety assessment forever, and continued supply without investigation can turn an engineering problem into a governance failure.

Component Suppliers — When the Defect Starts Further Upstream

A finished product can fail because of something its brand owner never manufactured. Batteries, airbags, printed circuit boards, fasteners, resins, coatings, sensors and software modules may originate several tiers upstream. Yet, their performance is part of the integrated product's safety. Supplier approval, therefore, requires more than price and delivery assurance: purchasers require specifications, process controls, traceability, change notification, and evidence that critical components have been tested under conditions the finished design creates.

The DVSA's vehicle-recall code expressly anticipates that problem. Where a safety defect involves a third-party component supplier, producers should identify that supplier and, where known, inform DVSA if other producers use the same component, so that DVSA can track the

issue across the wider market. Product-liability law likewise recognises component complexity: a component producer has a defence where a defect is wholly attributable to the subsequent product's design or to instructions from its producer.

CASE STUDY

Takata airbags illustrate the potential scale of a single upstream defect. A UK Citroën C3 safety recall recorded in March 2025 covered 55,166 vehicles because chemicals in affected Takata airbags could deteriorate over time, allowing the inflator to rupture and cause serious injury. Owners were told to stop using affected vehicles when safe to do so until replacement. One supplier's ageing mechanism can therefore create long-tail recall obligations for multiple vehicle manufacturers and distributors.

The Importer — More Than a Logistics Function

Importing is not simply a freight, customs or purchasing function. An organisation that brings regulated goods into Great Britain can become an importer with legal duties to verify that the manufacturer has completed the required conformity assessment, prepared the required technical documentation, and applied the appropriate markings. Government guidance expressly warns that businesses bringing products from the EU into Great Britain are now likely to be importers rather than distributors, carrying additional responsibilities.

The practical consequence is that an importer cannot safely rely on a supplier's reassurance that a product is "CE approved" or "UK compliant". Depending on the applicable legislation, it may need to verify manufacturer details, declarations of conformity, markings, instructions and traceability before placing goods on the market. If it has reason to believe a product is non-compliant, corrective action may include bringing it into conformity, withdrawing it, or recalling it entirely.

CASE STUDY

Diva Gift Limited provides a useful example of enforcement directly reaching an importer. The company imported a children's musical crib toy from a supplier in China and sold it through eBay. OPSS testing found detachable small parts creating a high choking risk to children under 36 months. In March 2024, Northampton Magistrates' Court imposed a £10,000 fine, £4,393.16 in costs and a £2,000 victim surcharge, resulting in a total payable of £16,393.16.

Recent border interventions show why documentary checking matters before commercial release. In August 2026, OPSS rejected a DayPlus rechargeable polishing machine because its Declaration of Conformity did not match the product, valid technical documentation was absent, and the charger failed an electrical-strength test, creating a serious electric-shock risk. A Hengjian off-road motorbike was rejected the same month after similarly inadequate conformity evidence left a serious fire risk unresolved.

Importer responsibility is therefore a governance issue as much as a regulatory label attached to a shipment. Procurement teams need to identify who is importing, which market is being entered, which legislation applies, and what evidence must be in place before goods are released. Contracts should require complete technical documentation, valid declarations, traceability, and cooperation in recalls, but contractual promises do not replace the statutory checks that the importer itself must perform.

The Distributor — The Duty Not to Look the Other Way

Distributors occupy the middle of the chain, but their position does not make them invisible to product-safety law. Under the General Product Safety Regulations 2005 in Great Britain, a

distributor must act with due care, must not supply a product it knows or ought to know is dangerous, should pass on risk information, retain traceability records and cooperate with enforcement authorities when investigation, withdrawal or recall becomes necessary for a particular product line.

That duty requires proportionate verification rather than laboratory re-engineering of every product a distributor handles. A distributor should recognise obvious non-compliance, check relevant markings and instructions, preserve information identifying its supplier, and react to alerts, recalls or credible complaints. Storage and transport also matter: damaged packaging, excessive heat, moisture, impact, contamination or poor battery handling can turn an originally compliant product into an unsafe one before it reaches the retailer.

OPSS action against Desertcart in January 2024 shows that downstream status offers little shelter once a serious hazard is known to exist. The regulator served a Withdrawal Notice regarding UPP model U004 and U004-01 e-bike batteries, which present a serious fire risk. Desertcart, identified as the distributor, was required to withdraw the batteries from sale and contact all purchasers, illustrating how responsibility can crystallise after a product has already entered distribution.

The central question is therefore what a competent distributor knew, should have known and did after receiving relevant information. A suspicious certificate, repeated returns, damaged stock or a regulator alert should trigger an investigation rather than routine resale. Commercial pressure to clear inventory cannot override safety duties. Distributors that maintain reliable supplier records, quarantine procedures, recall contacts and escalation routes are better placed both to protect customers and to demonstrate due care.

The Retailer — The Final Gatekeeper

Retailers are the final commercial gate before many products reach consumers, and they often receive the earliest evidence that something is wrong. Government guidance states that sellers must not supply consumer products they know or should have known to be unsafe. Retailers need supplier records sufficient to support traceability. They should report safety risks or consumer incidents to the manufacturer, supplier, or the relevant Trading Standards service rather than treating complaints as customer service matters.

The retailer's advantage is proximity to real-world use of the finished product. Returns, complaints, photographs, warranty claims, and staff observations can reveal patterns that are invisible during pre-market testing. A single broken plug may be accidental; repeated reports of overheating across a model may indicate a systemic defect. Effective retailers therefore aggregate safety-relevant complaints rather than closing each transaction separately, since fragmented data can hide the early warning signs of an emerging recall.

Retail obligations also overlap with consumer law more broadly. Under the Consumer Rights Act 2015, goods supplied by a trader to a consumer must be of satisfactory quality, fit for particular purposes made known to the trader and as described; safety forms part of satisfactory quality. A retailer may therefore owe the consumer a remedy even when the defect originated overseas, while recovery against upstream suppliers remains a separate commercial exercise entirely.

Large retailers can use purchasing scale as a genuine safety control. Supplier onboarding may require test reports, declarations, technical files, approval of manufacturing sites, product change notifications and cooperation in recalls before a listing is authorised. Surveillance can then combine customer complaints, return rates, regulator alerts and periodic sampling. A defective private-label line may expose the retailer not only to refunds and reputational damage, but also to producer-level liability where branding changes legal status.

The strongest retailer response is therefore neither blind reliance on upstream certification nor an attempt to duplicate the manufacturer's engineering function. It is a disciplined gatekeeping system that asks whether the evidence is credible, whether complaints suggest an emerging

risk, and whether continued sale remains defensible. Immediate quarantine, listing suspension and escalation may prevent a small defect population from becoming a national recall, provided the retailer's systems are actually listening for it.

Own-Brand Products and Private Labels

Private-label sourcing can transform a purchaser into something closer to a producer in law. Under the Consumer Protection Act 1987, liability can attach to a person who puts its name, trade mark or other distinguishing mark on a product and thereby holds itself out as the producer. The commercial attraction of own-branding carries a corresponding legal consequence: customers may be entitled to look directly to the brand owner when the product is defective.

The same principle appears across modern regulatory regimes. Government guidance on consumer connectable products states that an organisation marketing a product made by another person under its own name or trademark is treated as a manufacturer for the purposes of those security requirements. RoHS guidance similarly provides that an importer placing electrical or electronic equipment on the market under its own name or trademark must comply with manufacturer obligations, so rebranding changes regulatory status, not merely packaging.

For procurement teams, private-label governance should therefore resemble manufacturer oversight rather than ordinary resale. Specifications, approved factories, component controls, testing rights, change notification, technical documentation and recall cooperation become critical because the brand owner has deliberately placed its identity between the factory and the customer. A strong indemnity may recover some upstream losses, but it cannot undo reputational damage or prevent statutory liability once legislation treats the own-brander as producer or manufacturer.

Overseas Manufacturers and Complex Global Supply Chains

Global sourcing can place the physical manufacturer several contractual steps and thousands of miles away from the eventual customer. That distance complicates inspection, enforcement, service of proceedings, evidence preservation and recovery. A UK purchaser may buy from a domestic distributor that sourced through an importer, trading company or marketplace seller. At the same time, the factory itself has no UK assets, so product safety depends heavily on establishing a responsible economic actor within practical regulatory reach.

The scale of border intervention shows why that matters so much in practice. During 2025-26, OPSS-supported checks covered 11,310,080 goods entering the UK; 345,919 were determined unsafe, and 2,397,013 were non-compliant, for a combined total of 2,742,936. OPSS estimated that preventing those goods from entering circulation avoided about £81 million of detriment associated with unsafe products and approximately £209 million associated with non-compliant products entering the market.

Direct-to-consumer e-commerce weakens the traditional assumption that a UK importer will always stand between an overseas factory and the buyer. The Government's 2026 proposals expressly identify difficulties taking action against overseas sellers and the sheer volume of non-compliant products entering through online and international supply chains. Proposed rules would therefore make the overseas seller itself the producer in certain distance-sale situations where no UK manufacturer, authorised representative, or importer exists.

The September 2026 FREESKY 540E electric-bicycle intervention illustrates the practical problem well. OPSS rejected the import after finding that a valid Declaration of Conformity had not been supplied and that there was no evidence of relevant UK conformity assessment; inadequate labelling also remained. The product, manufactured by Guangzhou Electroy Corporation in China, was assessed as presenting a serious fire risk because conformity of the electrical system could not be demonstrated to regulators.

Supply-chain contracts should therefore establish more than just price, Incoterms, and

delivery dates. Buyers need factory identity, manufacturing location, access to technical files, component traceability, audit rights, change controls, insurance evidence and enforceable cooperation obligations. Where the manufacturer sits beyond easy jurisdictional reach, the solvency and responsibilities of the UK importer or distributor become commercially important, since a low purchase price can prove illusory if recovery after a national recall depends on an inaccessible counterparty.

Fulfilment Providers, Warehouses and Logistics Operators

Fulfilment providers occupy an increasingly important position between online sale and physical delivery. They may warehouse, package, address and dispatch goods without owning them, giving them operational control but not necessarily conventional seller status. In Northern Ireland, the EU General Product Safety Regulation expressly recognises fulfilment service providers. The Government's 2026 Great Britain proposals likewise state that such businesses should fall within the proposed "onward supplier" category rather than sit entirely outside the safety chain.

That classification reflects practical influence over the product's condition. Warehousing can expose lithium batteries to heat, water or physical damage; repacking can remove warnings or batch information; labelling errors can send the wrong safety instructions to customers; and dispatch systems can continue shipping stock after a recall begins. A fulfilment operator may not have designed the product, but its processes can preserve, worsen or help control the risk once goods enter domestic distribution.

The boundary becomes particularly blurred where one organisation stores stock, prepares listings, packages orders, manages returns and handles customer communications for an overseas seller. Those activities generate information that can quickly identify unsafe products. Under the Northern Ireland GPSR, fulfilment service providers are an expressly recognised economic-operator category. At the same time, the proposed Great Britain framework would clarify their inclusion as onward suppliers, so regulatory attention follows operational control rather than ownership labels.

Contracts with logistics providers should accordingly contain product-safety controls alongside service levels for picking accuracy and delivery speed. Recall holds, serial or batch traceability, quarantine areas, damaged-stock procedures, controlled disposal and urgent data extraction can determine whether corrective action succeeds. If a warehouse can identify every affected unit within hours, recall costs and consumer exposure may be contained; if stock is commingled or records are weak, a manageable incident can expand rapidly.

Conformity Assessment and Product Certification

Conformity assessment is the process used to demonstrate that a product meets applicable legal requirements before it is placed on the market. Depending on the legislation and risk category, the manufacturer may self-declare conformity or may need an independent approved or notified body. The assessment can involve design review, type examination, testing, production-quality controls and documentation, and its purpose is evidential: it shows how specified requirements were addressed before goods are sold.

The process should not be confused with a general certificate of safety. Product legislation sets essential requirements concerning health, safety, performance or environmental protection, while standards provide technical routes for meeting some of those requirements. Government guidance is explicit that applying a standard does not replace legal obligations. A product can follow a relevant standard yet remain unsafe because another hazard falls outside its scope or because production no longer matches the design.

Assessment routes also differ significantly by product category. Many products can rely on manufacturer self-declaration, while higher-risk categories require third-party involvement. The Government's conformity-assessment database showed 173 UK approved bodies in September 2026, spanning multiple legislative areas, while the MHRA listed nine UK approved

bodies for medical devices in July 2026. An approved body's existence tells buyers little unless its designation covers the product, legislation and procedure concerned.

The declaration accompanying a product is equally important to the chain of evidence. It identifies the manufacturer, product, legislation, standards, and responsible signatory, creating a formal link between the marketed item and the assessment that underpins it. In August 2026, the Hengjian off-road motorbike was rejected at the border because its supplied Declaration of Conformity did not match the product, and OPSS found no valid technical documentation or production-control evidence, leaving a serious fire risk.

Conformity assessment is most effective when treated as a system rather than as a document requested at the end of procurement. Buyers should confirm the model assessed, applicable standards, laboratory scope, certificate validity, manufacturing location, and whether later component substitutions invalidate earlier evidence. A test of a single representative sample cannot indefinitely prove that every batch remains identical, so change control and ongoing production assurance are essential companions to initial certification, not optional extras.

The commercial lesson is that conformity evidence should answer a chain of questions: which legal requirements apply, which route was used, who performed independent work, which configuration was examined, and whether current stock still matches it. Missing links require investigation before acceptance. Certification can substantially reduce uncertainty, but it transfers no responsibility away from manufacturers, importers or purchasers whose own decisions determine whether credible evidence is obtained and acted upon.

UKCA, CE Marking and Recognised Standards

UKCA and CE markings indicate that the manufacturer claims the product meets applicable conformity requirements for the relevant market; neither is a general quality award nor a guarantee that failure is impossible. In Great Britain, continued recognition of current EU requirements, including CE marking, applies across 21 product regulations. UKCA remains available, while sector-specific arrangements differ for medical devices, construction products, marine equipment and transportable pressure equipment.

For many sectors of the Great Britain market, the 2024 amendments removed the previous 31 December 2024 expiry of CE recognition, allowing businesses to continue using recognised EU requirements alongside UKCA. That flexibility reduces duplicate assessment costs for organisations serving both markets, but it also makes regulatory checking more nuanced. Procurement teams cannot assume one mark answers every question; they must confirm sector, destination market, legislation, standards and assessment route.

Designated standards add a further layer of evidence. In Great Britain, a government-designated standard can create a rebuttable presumption of conformity with the essential requirements it covers. That presumption is limited: standards may address only part of the legislation, can be designated with restrictions, and never transfer responsibility away from the manufacturer. Following a standard is powerful evidence of compliance, but a real hazard can still rebut the assumption of compliance.

CE-marked goods placed on the Great Britain market under continued recognition may rely on EU harmonised standards, but the legal mechanics differ from UKCA. Guidance published in March 2026 explains that CE products following harmonised standards do not, by themselves, receive the Great Britain statutory presumption attaching to UKCA products that follow designated standards. The practical compliance outcome may still be acceptable, but the evidential routes remain distinct in law.

The safest procurement approach treats markings as the visible endpoint of an evidence chain, not the beginning and end of due diligence. Buyers should obtain the declaration, identify applicable legislation, verify approvals or notifications, review the standards, and confirm that the delivered model matches the assessed configuration. A perfectly printed CE or UKCA symbol on a non-compliant product is still only ink; lawful marking depends on the

conformity work behind it.

Testing, Certification and Third-Party Assurance

Testing converts design assumptions into evidence by measuring how a product performs under defined conditions. Depending on the risk, laboratories may assess electrical strength, flammability, mechanical loading, chemical composition, ingress protection, sterility or other characteristics. The value of the result depends on competence, method, sample selection and traceability. A technically impressive report provides weak assurance if the laboratory lacked relevant capability or the sample cannot be reliably linked to production stock.

Accreditation helps establish that competence exists in the first place. UK government policy recognises the United Kingdom Accreditation Service as the national accreditation body, describing accreditation as “checking the checkers” because it assesses organisations that perform testing, calibration, certification and inspection. In regulated sectors, approved bodies must also hold the appropriate appointment under the relevant legislation and product scope, so buyers should verify both accreditation and designation.

Third-party assurance still has real limits worth remembering. A laboratory usually reports what happened to defined samples using specified methods; it does not guarantee that every subsequent production unit is identical, nor does a certification body assume the manufacturer’s responsibility. Sampling can miss intermittent defects, counterfeit substitutions or process drift. For high-risk products, assurance should combine type testing with factory controls, batch testing where proportionate, supplier audits and complaint monitoring.

Independent evidence becomes most valuable when it challenges convenient assumptions. In August 2026, OPSS rejected the DayPlus rechargeable polishing machine after its charger failed an electrical-strength test and the supplied declaration did not match the product. The result did more than expose defective paperwork: physical testing identified a serious electric-shock hazard. Effective assurance therefore triangulates documentation, certification, and actual performance, rather than letting a single reassuring document silence contradictory evidence.

When the Certificate Is Wrong

Certificates fail in several different ways. Some are counterfeit; others are genuine but issued outside the body’s accredited scope, relate to a different model, cite an inappropriate standard or describe a sample no longer representative of production. UKAS states that it has identified several counterfeit certificates and false accreditation claims in circulation. Procurement assurance therefore requires independent validation of the issuer, accreditation, scope, certificate number and product identity, not a visual glance at a PDF.

CASE STUDY

Grenfell Tower remains one of the gravest examples of certification and assurance failure in UK history. The Inquiry’s 2024 Phase 2 report found that Celotex manipulated a 2014 fire test of its RS5000 insulation using concealed fire-resisting boards, while certification and approval processes surrounding Kingspan’s K15 product failed to expose deficiencies in supporting fire-performance evidence. Arconic likewise relied on test data concerning a more fire-retardant cladding variant than the panels ultimately supplied.

As of September 2026, the Grenfell Tower Inquiry had identified serious failings by testing and certification bodies, including BRE’s complicity in Celotex’s manipulated 2014 fire test. The Metropolitan Police had also confirmed that files concerning up to 57 individuals and 20 organisations would be submitted to the Crown Prosecution Service by 30 September 2026, with charging decisions expected before June 2027. For procurement teams, Grenfell shows that apparently authoritative certification can coexist with flawed, manipulated or misleading evidence.

Even authentic evidence ages in ways procurement teams often overlook. A report may concern an earlier factory, component, firmware version or standard, while production changes continue unnoticed downstream. UKAS accreditation schedules define exactly which activities an organisation is competent to perform, and its electronic certificates are meant to be read alongside those schedules. An impressive logo cannot extend the scope of accreditation, so buyers should compare dates, tested models, and current schedules before relying on historical assurances.

The 2026 border reports provide a more everyday warning of the same underlying problem. FREESKY, Hengjian and DayPlus products were rejected after declarations were either invalid or did not match the goods. At the same time, physical or documentary deficiencies left serious fire or electric-shock risks unresolved. The correct response to a doubtful certification is verification, not assumption: contact the issuing body, check official registers, inspect the scope and test reports, and quarantine stock where necessary until the issue is resolved.

Supplier Assurance — Trust but Verify

Supplier assurance begins with a simple proposition: evidence supplied by a manufacturer or distributor should be tested, not merely filed away. A declaration of conformity, laboratory report or certificate is useful only if it relates to the exact product being purchased, the correct legislation, the current manufacturing site and the present configuration. Purchasers should verify identifiers, dates, standards, issuing bodies and scope, then reconcile that evidence with the goods actually delivered.

Risk should determine the depth of assurance applied to any given product. Low-risk, established products may justify documentary checks and supplier declarations. Higher-risk electrical, construction, medical, or children's products may instead require independent testing, factory audits, batch sampling, or specialist technical review. The Government's 2026 proposals expressly contemplate additional verification duties for onward suppliers and online marketplaces for categories presenting significant risks, including checking declarations and conformity markings before supply.

Assurance should also examine the supplier's standing behind the paperwork itself. Accreditation schedules, approved-body designations, test-house competence, manufacturing capability, complaint history, and regulatory action can reveal weaknesses that are invisible in a certificate. A purchaser should ask whether the laboratory was competent for the specific test, whether samples were independently selected, and whether production has changed since testing took place. For critical products, audits should follow the process from incoming materials to release.

The strongest control available to procurement is triangulation across several independent sources. Procurement compares supplier documents with public registers and regulatory alerts; technical teams test whether standards and specifications are appropriate; quality teams inspect production evidence; and contract managers monitor complaints, substitutions and changes after award. Government guidance makes clear that manufacturers and importers remain responsible for safety after market placement. Trust remains commercially necessary, but verification turns trust into defensible assurance.

Traceability — Knowing Where the Product Came From

Traceability is the ability to connect a physical product with the businesses, places, batches and records that created and moved it. Government guidance recommends that products or packaging identify the manufacturer and importer, where applicable, together with a product or batch reference identifying the place and time of manufacture. Many sector regimes go further, requiring type, batch, or serial numbers and the retention of technical documentation for periods that commonly reach ten years.

The practical value becomes obvious when only part of a production run is affected by a fault. In August 2026, Bull Products and Cygnus Group recalled fire-alarm detection systems after

identifying a communication fault that could delay fire detection and alarm activation. The defect was confined to a single batch of network control units (reference 2410), and not every unit in that batch was affected, so batch traceability enabled targeted corrective action.

Good traceability links more than a serial number to a purchaser's name and address. It should identify manufacturing site, production date, critical components, supplier lots, inspection results, software or firmware version, distributor, customer and, where proportionate, installation location. That information allows investigators to ask whether failures cluster around one factory, one component batch, or one design revision, and it reduces the population that requires quarantine, testing, or recall when evidence supports a narrower group.

Traceability Beyond Tier One

Knowing the immediate supplier is only the beginning, since safety-critical components often originate deeper in the chain. A branded appliance may contain a battery cell from one country, a protection circuit from another, software from a third-party developer and a charger manufactured elsewhere. If the defect originates in any of those inputs, a purchaser recording only its Tier One distributor may struggle to identify other affected products, alternative sources or the true root cause.

The automotive sector particularly clearly demonstrates the scale of this upstream dependency. A single component can appear across several manufacturers, models and years, so recall systems need to follow component provenance rather than brand alone. UK vehicle-recall guidance expects producers to identify third-party component suppliers and, where known, tell DVSA if other producers use the same component, allowing a defect discovered in one vehicle population to trigger investigation across the wider market.

Construction products present a similar challenge because performance can depend on treatments, coatings, fixings and subcontracted processes rather than the base material alone. In 2025-26, OPSS investigated fire-rated plywood after concerns raised by the London Fire Brigade and found assurance gaps where manufacturers subcontracted the fire-retardant treatment. Four Prohibition Notices were served, halting supply and requiring recalls; OPSS noted that enhanced products commonly cost two to three times as much as standard plywood.

Traceability beyond Tier One therefore requires genuine contractual flow-down, not just a supplier list. Tier One suppliers should identify critical sub-suppliers, notify of changes, maintain batch genealogy, and preserve evidence linking components to finished products. Purchasers may also need audit rights or direct access to technical information where risk justifies it, since a supplier can otherwise change a cell manufacturer, resin formulation, software library or subcontractor. At the same time, the catalogue number remains the same throughout.

Digital systems can strengthen this chain by linking serialised finished goods to bills of materials, supplier lots, test results and revisions. However, technology cannot automatically repair weak governance. Data standards must be consistent, identifiers must survive repacking, and records must remain accessible after suppliers merge, fail or change systems. The value lies in reconstructing the product's history quickly enough to support containment, root-cause analysis, and targeted corrective action.

The commercial objective is not unlimited visibility into every commodity a business handles. It is risk-based visibility to the point where a plausible safety failure can be traced to its origin and contained. Safety-critical batteries, structural fixings, flame-retardant treatments, pressure components and software modules generally justify deeper provenance than packaging or decorative inputs, so procurement should direct the greatest scrutiny towards components whose failure could cause serious harm to someone.

Technical Files and the Product Safety Audit Trail

A technical file is the evidential history behind a product's claim to compliance. Depending on the applicable legislation, it may include design drawings, calculations, risk assessments, standards, test reports, bills of materials, conformity assessment evidence, declarations, instructions and production control information. Government guidance for many UKCA- and CE-regulated products requires that technical documentation be retained for the statutory period, typically 10 years after each product is placed on the market.

The file should evolve as the product itself evolves, rather than remain frozen at launch. Government guidance specifically warns economic operators to maintain procedures that preserve compliance when design, characteristics or relevant standards change. A supplier that substitutes a battery, modifies firmware or moves production to another factory may invalidate earlier testing even if the model name remains unchanged, so change-control records should explain what changed, who assessed the effect, and why continued supply was justified.

A defensible audit trail connects commercial and technical decisions across the whole lifecycle. Purchase specifications should match drawings; approved samples should match production; inspection records should identify batches; certificates should correspond to current components; and complaints should feed back into risk assessment. When an authority requests evidence, the organisation should reconstruct its rationale for compliance without relying on employees' memories, because technical files are the operating record, not archives.

Digital Product Information and the Future of Traceability

Product information is moving from static labels and paper manuals towards digital records accessible throughout a product's life. The Government's March 2026 consultation proposes a "digital by default" direction for the new Great Britain framework, allowing certain producer details, safety information and instructions to be supplied digitally. Physical identifiers would remain important, particularly batch or serial information, since a digital record still needs an unambiguous link to the product in front of the user.

The consultation envisages data carriers such as QR codes, with built-in safeguards for accessibility and durability. Where safety information is digital, the label should explain what can be accessed and that the information should be read before use. The Government proposes that digital information remain accessible for the product's expected lifetime, taking into account repair and refurbishment, recognising that ordinary webpages, hosting arrangements and domain ownership may disappear long before durable products do.

Construction-product reform is moving in the same direction. The 2026 Construction Products Reform White Paper proposes that product information should be available digitally, with unique product identifiers linked through digital labels such as QR codes. The accompanying general safety consultation explains that traceability is essential to corrective action and proposes that products include the manufacturer's identity, address, unique identifier and a data carrier, reflecting lessons from the post-Grenfell drive for reliable information.

Medical-device regulation offers another example of increasingly granular identification requirements. Draft reforms, consulted on by the MHRA in 2026, propose compulsory unique device identifiers and implant cards, intended to improve lifecycle traceability and the management of adverse events. Although medical devices sit within a specialist regime, the principle has wider relevance: reliable digital identity can connect a physical product to its manufacturer, configuration, safety notices, and maintenance history more precisely than a generic model name can.

Digitalisation also creates governance risks alongside its evident benefits. Information can be altered after sale, QR codes can be replaced, databases can become inaccessible, and cybersecurity failures can undermine trust in the record itself. Organisations therefore need controlled version histories, durable hosting, access rights and evidence showing what information was available at a particular time. The future of traceability is creating persistent,

authenticated product records, not simply moving existing paperwork online.

When Records Are Missing

Missing records can turn a contained technical problem into a much larger legal and operational one almost overnight. Without purchase orders, batch numbers, certificates, test reports or distribution records, an organisation may be unable to prove which specification applied, which units were affected or which customers received them. Government guidance requires sellers to keep records identifying suppliers, while many regulated regimes require manufacturers and importers to retain declarations for approximately ten years.

The immediate safety consequence is uncertainty that spreads outward from a single missing document. If a component batch is suspected but genealogy records are missing, unaffected products may need to be quarantined alongside defective ones. If customer records are incomplete, recall communications must rely more heavily on public advertising and retailer outreach. Lost evidence also hampers root cause analysis, since investigators cannot confidently compare production dates, suppliers, test results, or design revisions.

The legal consequence can be equally severe, as the PPE Medpro litigation shows. DHSC recovered £121,999,219.20 for non-compliant surgical gowns but failed on a separate £8,648,691 storage-cost claim. The High Court held that the storage loss had not been proved adequately: the supporting spreadsheet lacked sufficient underpinning and the witness presenting it lacked personal knowledge of its preparation. Records determine both quantum and technical liability in disputes of this kind.

Record retention should therefore be designed around foreseeable disputes, recalls and regulatory enquiries, not minimal administrative convenience. Organisations need controlled repositories, ownership rules, retention schedules and auditable links between contract, specification, batch and customer. Critical evidence should survive staff turnover, outsourcing and supplier insolvency. A document that cannot be located, authenticated or connected to the affected product is practically equivalent to no document at all when decisions must be defended years later.

The First Safety Incident

The first complaint should be treated as information, not dismissed merely because it is the first one received. The immediate task is triage: establish what happened, identify the exact product and batch, preserve the item where possible, record photographs and circumstances, assess injury or property damage, and determine whether similar reports exist. A rapid initial assessment should distinguish routine quality dissatisfaction from a plausible safety event without assuming one incident proves a systemic defect.

Containment may need to begin before root cause is fully known or understood. Suspect stock can be quarantined, dispatches paused, marketplace listings suspended and replacement batches held while technical investigation proceeds. These actions are reversible if the concern proves unfounded; continued supply may not be reversible if further injuries occur. Organisations should define in advance who has the authority to stop distribution, since hesitation due to unclear approval routes can turn a question into exposure.

Evidence must be preserved immediately, before memories fade or components are discarded. The failed product, packaging, charger, instructions, photographs, purchase records, software version and environmental conditions may all matter. Investigators should avoid destructive testing until an evidence plan has been agreed where litigation is foreseeable. Supplier notifications should request the corresponding production and test records without encouraging the alteration of documents, thereby creating a contemporaneous record that can support technical conclusions and later proceedings.

Haier's heat-pump tumble-dryer incident shows the depth a serious investigation can require in practice. In May 2025, OPSS declared a national incident involving more than 103,000 dryers presenting a fire risk. Enforcement officers, scientists, engineers and risk assessors

reviewed technical documentation and examined products in OPSS laboratories. The regulator concluded that deteriorating wiring around compressor pipework containing flammable refrigerant was the root cause, and found the manufacturer's initial modification unsatisfactory.

The first incident should also trigger a deliberate search for weak signals elsewhere in the business. Warranty returns, customer service notes, repair reports, social media complaints, insurer notifications and distributor feedback can reveal earlier events that were individually misclassified. The Vauxhall Zafira investigation illustrates the danger of fragmented signals: Parliament concluded that Vauxhall had been too slow to investigate a distinctive pattern of fires and too quick to attribute them to unauthorised repairs.

Senior escalation should depend on both potential severity and incident count, not on either alone. A single credible report involving fire, electrocution, structural failure, poisoning or a vulnerable child can justify executive attention before statistical certainty exists. The first hours should establish ownership across the safety, quality, legal, procurement and communications functions, identify notification obligations, and set decision checkpoints, since disciplined documentation matters as much as speed.

Product Safety Risk Assessment

Risk assessment translates technical evidence into a decision on which action is proportionate to the hazard. OPSS's Product Safety Risk Assessment Methodology, PRISM, is used by Great Britain's market-surveillance authorities for general non-food consumer products and aligns with the EU Safety Gate approach. It considers injury scenarios, severity and probability to reach a risk level, though businesses using comparable reasoning should avoid treating any numerical score as a substitute for expert judgement.

Exposure matters alongside probability in ways that are easy to underestimate. A rare failure in ten units may pose a different societal risk from the same failure rate across one million units. At the same time, the consequences differ sharply between minor irritation and a fatal fire. Vulnerable users can change the assessment because children, older people or people with disabilities may be less able to recognise hazards or escape them once a failure actually occurs.

The 2025-26 Product Safety Database demonstrates the range of risk levels regulators encounter in ordinary practice: 563 notifications were recorded as serious risk, 259 as high, 127 as medium, and 229 as low, while 1,074 had no assigned risk level at the time of notification. Fire was the most frequently recorded harm among unsafe or unsafe-and-non-compliant notifications, appearing 424 times, reinforcing the case for risk classification being evidence-led and open to revision.

Corrective Action — Repair, Warning, Withdrawal or Recall?

Corrective action should remove or reduce the risk with the least possible delay, but the appropriate measure depends on where affected products are and how serious the hazard is. A manufacturing adjustment may address unsold stock; a warning may manage a limited residual risk; withdrawal removes products from distribution channels; and recall seeks products already supplied to end users. Government guidance also recognises modification and new instructions as possible responses where they genuinely restore safety.

The distinction between withdrawal and recall is operationally important in practice. Withdrawal can prevent remaining stock from reaching consumers, while recall reaches back into homes, workplaces or installed environments. During 2025-26, the Product Safety Database recorded 249 withdrawals and 479 recalls from end users, along with 150 actions to bring products back into compliance and 71 modification programmes, so corrective action is not binary but a spectrum matched to risk.

Bull Products and Cygnus Group provide a recent example of layered action working as intended. After a fault was identified in a batch of fire-alarm network control units, remaining

stock was quarantined, affected products were withdrawn, and a phased replacement programme began for all affected units, including those not yet exhibiting failures. The business also introduced enhanced end-of-line testing and redesigned the control board, addressing customers, inventory and recurrence together rather than only the symptom.

Haier's heat-pump case shows how a first response can be found wanting and escalated further. OPSS concluded that Haier's initial modification solution was unsatisfactory and issued a formal Notice to Warn, after which a revised modification programme was initiated for the affected population. Regulators can require stronger action wherever voluntary measures prove insufficient, and this case demonstrates that a modification programme is not necessarily the end of the corrective-action story.

The decision should be documented as carefully as the underlying technical investigation itself. Records should explain affected populations, risk classification, options considered, expected effectiveness, treatment of vulnerable users, regulator input and monitoring arrangements. Corrective action also requires exit criteria: organisations should know when a recall has reached an acceptable level of effectiveness or when additional outreach is required, since the strongest response is to remove the hazard and prevent the same failure from entering future production.

Product Recalls — Who Pays?

A recall incurs costs far beyond simply replacing the defective item itself. Businesses may need customer identification, call centres, postage, engineers, collection, warehousing, refunds, replacement stock, disposal, laboratory testing, legal advice, advertising and additional logistics. Retailers and distributors may incur their own handling costs before seeking upstream contractual recovery. Product-recall insurance can cover specified exposures, but scope, deductibles and exclusions matter, and contractual indemnities redistribute cost without removing regulatory responsibility.

Whirlpool's washing-machine recall illustrates the scale such programmes can reach in customer-processing terms alone. By October 2021, 277,715 potentially affected customers had come forward, 209,956 affected-machine cases had been fully resolved, and 201,237 machines had been replaced free of charge. Whirlpool reported 3,359,301 visits to the recall website, while only 47% of the estimated 590,000 potentially affected machines had been registered at that point, underscoring how costs grow with both scale and the difficulty of locating users.

Who ultimately pays depends on legal rights and commercial leverage, not who caused the defect. A retailer may refund the consumer but recover against its distributor; an importer may pursue the manufacturer; insurers may exercise subrogation; and liability caps or exclusions may restrict recovery between businesses. Insolvency can leave costs stranded downstream: a June 2026 UK recall of UNU electric mopeds noted that the manufacturer, UNU GmbH, had entered insolvency, leaving owners directed to safe disposal.

Notification to Regulators

Notification is not optional once the statutory threshold has been met. Under the General Product Safety Regulations 2005 in Great Britain, producers and distributors that know a product they supplied poses risks incompatible with the general safety requirement must immediately notify the relevant enforcement authority in writing. Government guidance states that this will normally be the local Trading Standards authority, although sector-specific products may fall to OPSS, HSE, MHRA, DVSA or another regulator.

A serious-risk notification should contain enough information for authorities to act on straight away. Government guidance requires precise product identification, a full description of the risk, available traceability information and details of measures already taken to prevent harm. The Product Safety Database captures information such as importer details, batch numbers, test reports and corrective actions. Hence, a vague statement that "an issue is under

investigation” is no substitute for structured evidence.

Timing matters because notification and corrective action often occur simultaneously rather than in sequence. Businesses should not wait for perfect root-cause certainty when they already know that a supplied product is unsafe, and initial information can be updated as testing progresses. The 2026 business-notification guidance covers both consumer and non-consumer products across Great Britain and Northern Ireland, though the legal routes differ depending on the market and sector involved.

Different regimes impose additional notification duties on top of the general safety requirement. Consumer connectable-product security rules require manufacturers, importers and distributors to notify specified persons, including OPSS, of certain compliance failures, and to investigate and act on failures they know or ought to know about. In Northern Ireland, the EU General Product Safety Regulation requires notifications of dangerous products to be submitted through the Safety Business Gateway. Hence, a single reporting route rarely covers every incident.

Regulators can demand continuing information well after the first report has been submitted. Under the General Product Safety Regulations 2005, an enforcement authority can require regular progress updates by way of a formal information notice, and failure to comply without reasonable cause can itself be a criminal offence. Reporting obligations therefore extend beyond announcing the defect: authorities may expect evidence on consumer contact, remediation rates, outstanding populations and whether the chosen measure is actually working.

Good governance makes notification a rehearsed process rather than an improvised one under pressure. Organisations should maintain regulator contacts, templates, escalation thresholds, responsible officers and legal review arrangements before an incident occurs. The purpose is not to delay reporting through bureaucratic processes, but to ensure that accurate technical, commercial, and traceability information can be assembled quickly. An organisation unable to identify its regulator or affected batches within days has already revealed weaknesses in its management.

Crisis Management and Consumer Communication

A serious product-safety event rapidly crosses organisational boundaries within any business of scale. Engineering investigates root causes, quality control inspects stock, procurement engages suppliers, legal teams manage liability and privilege, customer service handles incoming reports, communications teams issue warnings, and senior management decides on risk appetite and resources. These functions must operate from a single verified incident picture, since contradictory messages can undermine both consumer action and regulatory confidence.

Consumer communication should be specific enough to drive behaviour rather than merely inform. Messages need to clearly identify affected products, explain the hazard in understandable language, state whether use must stop immediately, and provide a simple remedy. Model names alone may be insufficient where ranges contain both safe and unsafe variants, so photographs, batch numbers, purchase periods and serial-number checkers can improve identification, while contact routes must handle the surge created by national publicity.

Whirlpool demonstrates the scale of outreach required when products have been in homes for years before a recall reaches them. Following Government intervention in June 2019, 140,151 additional tumble-dryer customers came forward, and the dedicated website received more than 1.4 million visits by October 2021. OPSS required wider publicity and improved outreach to vulnerable consumers, showing that publishing a recall notice is only the beginning of a much longer communication effort.

Communication also needs credibility when the underlying evidence changes mid-recall. Haier’s 2025 heat-pump tumble-dryer incident required OPSS to advise owners of more than

103,000 affected machines to stop using and unplug them pending repair. Following a technical investigation, OPSS concluded that Haier's initial modification was unsatisfactory and issued a formal Notice to Warn. After that, a revised modification programme began, so crisis plans must accommodate changing conclusions without earlier messaging becoming an obstacle.

The best governance structure establishes an incident leadership team with clear decision rights, documented meeting records, and a single agreed-upon source of truth. Boards or executives should receive concise information on hazards, affected populations, regulator engagement, injuries, corrective actions, customer reach, supplier recovery and financial exposure. Communications should be tested against what recipients need to do, not what the organisation wishes to say, because in a safety crisis clarity and speed are themselves control measures.

The Cost of Acting Too Late

Delay allows exposure to accumulate in ways that are rarely visible until much later. Every additional unit sold, installed or used after credible warning signs appear can increase the eventual recall population, the number of incidents, and the remediation cost, and it can weaken legal arguments that reasonable care was taken. Product-safety governance therefore has to distinguish uncertainty from inaction, since organisations can still quarantine stock, suspend sales or notify regulators while evidence develops.

CASE STUDY

Vauxhall's Zafira B experience is a stark example of that distinction being missed at the time. The company sold 234,938 affected-model vehicles with manual or no air conditioning between 2005 and 2014. By 2015, a distinctive fire pattern had emerged; the London Fire Brigade reported 120 Zafira fires since 2013. Parliament later concluded that Vauxhall had been too slow to begin a full investigation and too quick to attribute the problem to unauthorised repair.

Whirlpool provides an even more striking illustration of long-tail escalation over a decade or more. Around 5.3 million affected tumble dryers had been manufactured for the UK market, with at least 750 lint-related fires reported to Parliament. The issue was notified to the Primary Authority in August 2015. Yet, OPSS announced its intention to compel recall only in June 2019, by which time as many as 500,000 unmodified machines were still potentially in use.

The cost of delay is therefore measured in more than just pounds sterling. It includes additional injuries, emergency service incidents, customer anxiety, executive distraction, regulatory intervention, litigation, lost sales and damaged confidence in brands or public bodies. Financial consequences eventually follow through replacement, storage, destruction, legal costs and supplier disputes, but the most important loss may be preventable harm, which no subsequent settlement or insurance payment can ever fully undo for those affected.

Summary — Safety Is a Supply Chain Responsibility

Product safety is no longer confined to the factory floor or the final inspection before goods are released. Modern products pass through complex networks of designers, component suppliers, manufacturers, importers, distributors, retailers, fulfilment providers and digital marketplaces. Each participant can influence whether a product remains safe, compliant and traceable, so when failures occur, responsibility may arise at several points simultaneously through regulation, contract, negligence or statutory product liability law.

The legal framework reflects that complexity by design, not by accident. The Consumer Protection Act 1987 provides strict liability for defective products in Great Britain, while negligence and contract law remain important where fault, specifications or commercial obligations are disputed. Sector-specific legislation, the General Product Safety Regulations

2005 and the Product Regulation and Metrology Act 2025 add further layers, so compliance depends on identifying which duties apply to each product and economic actor.

Conformity assessment, testing and certification provide essential evidence, but none should be treated as a guarantee of safety on its own. UKCA and CE markings indicate compliance with applicable requirements, not that every unit is defect-free, and certificates can be outdated, inappropriate, or fraudulent, as Grenfell demonstrated on a devastating scale. Effective supplier assurance therefore depends on verification, traceability, independent scrutiny where proportionate, and continuing control over components, factories and technical documentation.

Traceability becomes critical once a defect is suspected anywhere in the chain. Batch numbers, serial numbers, supplier records, technical files, inspection reports and component provenance allow organisations to identify affected products, isolate root causes and limit recalls. Weak records create the opposite effect: uncertainty expands the population that may require withdrawal or replacement, increases remediation costs and weakens legal evidence, so product-safety information must remain accessible long after the original procurement decision.

When an incident occurs, speed and judgement matter more than either alone. Businesses must preserve evidence, assess severity and probability, identify vulnerable users, determine whether continued supply is defensible, and choose among warning, repair, withdrawal or recall. Whirlpool, Vauxhall, Haier, Grenfell, and other cases discussed throughout this article demonstrate how delayed investigation or incomplete corrective action can magnify consumer exposure, regulatory intervention and reputational damage far beyond the original defect.

The central lesson is that safety cannot be delegated upstream or assumed from paperwork alone by any single actor. Manufacturers must control design and production; importers must verify compliance; distributors and retailers must respond to warning signs; purchasers must test supplier assurance; and every organisation needs systems capable of identifying, tracing and correcting risk. Product safety is best understood as a continuous supply-chain responsibility, extending from specification and sourcing through to eventual recall.

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

- Consumer Protection Act 1987
- Consumer Protection (Northern Ireland) Order 1987
- Sale of Goods Act 1979
- Consumer Rights Act 2015
- General Product Safety Regulations 2005 (SI 2005/1803)
- Regulation (EU) 2023/988 on General Product Safety, as applied in Northern Ireland
- Product Security and Telecommunications Infrastructure Act 2022
- Product Regulation and Metrology Act 2025
- The Noise Emission in the Environment by Equipment for Use Outdoors (Amendment and Transitional) Regulations 2025
- Directive (EU) 2024/2853 on liability for defective products

- *Building Safety Act 2022*

Case Law

- *Donoghue v Stevenson* [1932] AC 562
- *A v National Blood Authority* [2001] 3 All ER 289
- *Abouzaid v Mothercare (UK) Ltd* [2001] EWCA Civ 348
- *Wilkes v DePuy International Ltd* [2016] EWHC 3096 (QB)
- *Gee v DePuy International Ltd (The DePuy Pinnacle Metal on Metal Hip Litigation)* [2018] EWHC 1208 (QB)
- *Hastings v Finsbury Orthopaedics Ltd and Stryker UK Ltd* [2022] UKSC 19
- *Secretary of State for Health and Social Care v PPE Medpro Ltd* [2025] EWHC 2486 (Comm)

Official Reports, Regulatory Guidance and Consultations

- Office for Product Safety and Standards, “OPSS Delivery Report 2025-2026”, GOV.UK
- Office for Product Safety and Standards, UK Product Safety Database, annual statistics 2025-26
- Department for Business and Trade, “The UK’s New Product Safety Framework”, consultation, March 2026
- Department for Business and Trade, market surveillance and enforcement consultation, March 2026
- Department for Business, Innovation, Science and Trade / Ministry of Housing, Communities and Local Government, Construction Products Reform White Paper, 2026
- Grenfell Tower Inquiry, Phase 2 Report, September 2024
- Medicines and Healthcare products Regulatory Agency, consultation on unique device identification, 2026
- Driver and Vehicle Standards Agency, code of practice on vehicle safety recalls
- UK Accreditation Service (UKAS), guidance on accreditation and the identification of counterfeit certificates
- Office for Product Safety and Standards, guidance on UKCA and CE marking

Further Reading

- Christopher Hodges, “European Regulation of Consumer Product Safety” (Oxford University Press)
- Simon Whittaker, “Liability for Products: English Law, French Law and European Harmonisation” (Oxford University Press)
- Michael Jones and Anthony Dugdale (eds), “Clerk & Lindsell on Torts”, chapter on product liability (Sweet & Maxwell)
- Grenfell Tower Inquiry, published reports and evidence, grenfelltowerinquiry.org.uk
- GOV.UK, “Placing manufactured goods on the market in Great Britain” guidance
- GOV.UK, Office for Product Safety and Standards, www.gov.uk/government/organisations/office-for-product-safety-and-standards