The 95 risks and the supply chain

How the Cabinet Office National Risk Register 2026 reaches a company, and what to do about it under supplier risk and tiering.

> Every risk in the register comes with a reasonable worst case attached. That single design decision changes the question a business should be asking from **how likely is this** to **if it were happening now, would we know**.

1. WHAT CHANGED IN 2026

The Cabinet Office published the National Risk Register 2026 on 14 July 2026. It now carries **95 risks across nine themes**, up from 89. Seven risks were added and one, disruption of Russian gas supplies to Europe, was removed as reliance on those imports fell away.

ADDED IN 2026	THEME	WHY IT WAS ADDED
Cyber attack or disruption on data infrastructure	Cyber	Concentration of national activity in a small number of data centres and cloud regions
Digital resilience failure	Cyber	A failed update or dependency can take systems down worldwide with no attacker involved
Cyber attack on water infrastructure	Cyber	Control systems in a sector the register already rates at the top for impact
Cyber attack on police systems	Cyber	Degraded policing has second order effects on everything that depends on it
Significant disruption of the criminal justice system	Societal	Capacity pressure, including prison overcrowding
Threats to democracy from interference	State threats	Interference in the democratic process and in election infrastructure
Accidental damage on the National Gas Transmission Network	Accidents and systems failures	Agricultural and construction digging strikes on transmission pipelines

More than half of the additions are cyber or digital. Two risks now sit at the top of the published matrix for both likelihood and impact: **pandemic** and **water infrastructure failure or loss of drinking water**. Terrorist attacks in publicly accessible locations carry the highest likelihood rating in the register.

2. THE QUESTION THE REGISTER ACTUALLY ASKS

A likelihood rating invites a probability argument. A reasonable worst case does not. It hands you a scenario, fully specified, and the only useful response is operational: if that were running right now, would we know?

That question is harder than it sounds and much cheaper to answer than most resilience work. It does not need a threat intelligence function or a new platform. It needs a named piece of evidence per scenario, an owner, and a date it was last looked at. Where those three exist, the risk is watched. Where they do not, the risk is a blind spot, and no amount of policy documentation changes that.

3. WHY THE REGISTER IS HARD FOR A COMPANY TO USE

Almost none of the 95 land on you directly

A cyber attack on water infrastructure does not attack your company. It attacks a utility, which stops a supplier's process, which stops a delivery you were counting on. The register describes the event; the company experiences the transmission.

Ninety five scenarios against a supplier book is not a manual exercise

A hundred suppliers against 95 risks is 9,500 judgements. Done by hand, once, in a spreadsheet, it is out of date the week a supplier changes sector, loses its second source or gains a system integration.

Uniform exposure destroys the signal

Every company in the country is exposed to a pandemic and to loss of drinking water. Saying so about all of your suppliers tells you nothing useful.

What discriminates is the supplier

Whether it holds a live connection into your estate, whether it is your only source, which sector it trades in, how far its goods travel.

4. THE TRANSMISSION MODEL

Treat a national risk as something that travels down a channel into a supplier and out the other side as a supply failure. There are seven channels, and every risk in the catalogue names the ones it uses.

CHANNEL	WHAT IT CARRIES	WHAT MAKES A SUPPLIER A STRONG CARRIER
Systems and connectivity	Cyber and digital risks	A live integration into your estate, or virtual access
Power, water and telecoms	Utility and infrastructure failure	Energy or water intensive sectors
Movement of goods	Transport, port, fuel and route risks	Hauliers, wholesalers, long lead times
Physical site availability	Attacks, fires, floods, exclusion zones	Sole source, or a supplier with physical access to you
Workforce availability	Health, industrial action, displacement	Labour intensive sectors
Price, demand and market access	Conflict, sanctions, commodity shocks	Sole source or critical criticality
Regulatory and legal action	State action, licensing, enforcement	Regulated sectors

This is the whole trick, and it is deliberately dull. A risk with no channel into a supplier is not that supplier's risk. A risk with a strong channel is, whatever the supplier's questionnaire says.

5. WHAT WAJD FORGE DOES WITH IT

5.1 The catalogue

All 95 risks ship in the product, across the nine themes, each with:

- likelihood and impact on the register's 1 to 5 scale
- a one line reasonable worst case
- the channels it travels down and the sectors it hits hardest
- a detection line: what would show it first, in supply chain terms

The seven 2026 additions and the risks the register calls out at the top of its matrix carry the published position. The remainder are Forge's mapping of the register's structure into supply chain terms: the theme and

the risk are the register's, the rating and the wording are ours until a risk owner confirms them against the published document, which takes two clicks in the product. The board shows how many are confirmed, so nobody mistakes a mapped rating for a published one.

5.2 Exposure, per supplier

For each supplier, Forge computes how strongly it carries each channel from the supplier's own record: criticality, sole source, sector, access type, integration depth, lead time. Every risk is matched to the strongest channel it can use into that supplier, scaled by whether the risk names that supplier's sector and by how critical the supplier is to you. The score is the worst reachable risk, plus the next four closing half of the remaining gap. Five severe risks is worse than one, but not five times worse, and no long tail can push a supplier to 100.

SUPPLIER PROFILE	EXPOSURE	BAND	WORST RISK IT CARRIES, AND THE CHANNEL
Standard, no sector, no access, short lead time	31.6	medium	Water infrastructure failure, via utility
Standard packaging supplier, physical site access	40.2	medium	Attacks on publicly accessible locations, via site
Integrated IT vendor, physical and virtual access	75.2	critical	Cyber attack on data infrastructure, via systems
Important haulier, 14 day lead time	75.3	critical	Attacks on transport systems, via logistics
Critical sole source food producer	86.2	critical	Water infrastructure failure, via utility

Two things matter here. The spread is wide, so the number ranks a book rather than colouring it all red. And every number decomposes: the screen names the risk, the channel and the weight, so a supplier manager can argue with it.

5.3 Where it lands in supplier risk and tiering

National exposure is not a separate report. It is wired into the risk engine that already runs the supplier book.

In the blended score

30 per cent quantified loss, 25 per cent operational signals, 18 per cent questionnaire assessment, 12 per cent concentration and 15 per cent national risk exposure, before the external signal uplift. Clean paperwork no longer hides a severe national risk arriving down a strong channel.

As its own strategy

One of six selectable methods in the risk lab, beside operational, questionnaire, FAIR style quantified loss, Kraljic tiering and the blend. It re-ranks the book by what the register can reach.

In the tiers

An active risk on a critical supplier makes it Tier 1 while it lasts. An active risk on any supplier it reaches materially makes it at least Tier 2. Exposure of 50 or more makes a supplier at least Tier 3. Standing the risk down reverses all of it.

In the assessment that goes out

A supplier carrying heavy exposure gets the national resilience assessment: which site stops first without power or water, how long you can supply without mains, how you would take our orders with your systems offline, and what would tell you within hours that it had started.

In the signal feed

Marking a risk active raises an external signal against every supplier it reaches materially, so it flows through the same path as a sanctions hit: it lifts the blended score and shows against the open orders exposed to it.

In the audit dossier

The supplier record handed to auditors carries the exposure, the five worst risks reaching you through that supplier, the channel each travels down, and which of them have no detection source named.

5.4 Posture and the blind spot count

Against each of the 95 risks, an organisation records a position: not tracked, watching, active or stood down, with an owner and a **detection source**, the named evidence that would show it first. A risk counts as answered when it has a source, a named owner and a review inside 180 days. Anything older is stale, and stale is not an answer.

A **blind spot** is a risk that reaches at least one supplier and has no detection source. The board counts them, lists them worst first, and puts the number next to the theme it sits in. This is the deliverable: not a heat map of the whole national register, but a short, ranked list of scenarios that can reach your business and that nobody is watching.

95	7	0%	10
risks held against the supply base	new entries carried at their published position	of the detection question answered on day one	blind spots on a first run, ranked worst first

Figures from a first run against a twelve supplier book with nothing configured. That is the honest starting position for most companies, and it takes an afternoon to move.

6. THE NEW CYBER RISKS, READ THROUGH A SUPPLY CHAIN

Cyber attack or disruption on data infrastructure

The worst case is a major data centre or cloud region going down for days, taking your order, stock and control data with it, and your suppliers' at the same time. The supply chain tell is distinctive: portal logins, order acknowledgements and integration calls stop together across suppliers who share one hosting provider, while suppliers on other platforms carry on. Forge routes this down the systems channel, so integrated and virtually connected suppliers carry it hardest.

Digital resilience failure

No attacker at all: a bad update or a failed dependency, as in the 2024 global IT outage. The tell is that failures arrive by vendor and version rather than by geography. Everyone on one platform stops; everyone else is fine. Most supplier questionnaires cannot see this, because they ask about controls rather than about concentration.

Cyber attack on water infrastructure

The register already rates loss of drinking water alongside pandemic at the top of the matrix. The cyber variant reaches a company through the utility channel into water dependent processes, which means food, pharmaceutical, chemical and paper suppliers before anyone else. The tell is that water dependent lines stop while power and telecoms at the same sites stay up.

Cyber attack on police systems

The addition companies dismiss fastest and should not. It reaches a business through vetting, clearances, site security cover and incident response times, all of which slip together and none of which show on a supplier scorecard.

7. WHERE THIS STOPS

Being clear about the boundary is what makes the rest usable.

- **Not a detection platform.** Forge does not read your endpoints, your firewall or your log platform. It watches the supply chain's behaviour: acknowledgement rates, integration heartbeats, lead time steps, delivery failures by region and by platform. For several of the 95 that is the earliest visible signal a company has, and for many others it is not. The detection source field exists precisely so the answer can name a tool Forge does not own.
- **Exposure is not a forecast.** It says what a risk can reach through a supplier, not that it will happen.
- **Ratings need confirming.** Ten of the 95 carry the published position. The rest are mapped, marked as such, and confirming one is recorded in the audit trail.
- **The scores are only as good as the supplier record.** A supplier with no sector, access type or integration recorded gets the base weights, which understates a supplier that is in fact deeply connected.
- **Nothing calls the internet.** The catalogue is data in the product, so it runs the same offline as online and can be amended per tenant.

8. A THIRTY DAY PATH

1. **Day one.** Open the national risk board. Read the blind spot list, not the 95.
2. **Days two to five.** Fill in access type, integration and sector on the top twenty suppliers by spend. This is the input that makes exposure discriminate.
3. **Week two.** Take a position on the ten risks that reach your book worst first. For each, name one piece of evidence that would show it first, and one owner. Watching with a named source beats active with none.
4. **Week three.** Send the national resilience assessment to every supplier over 50 exposure. Read the answers to the last two questions first.
5. **Week four.** Confirm the ratings you disagree with against the published register, then review the tier movement. Anything that moved to Tier 1 or Tier 2 on national exposure alone is a conversation you were not having a month ago.

The short version. The register gives you 95 fully specified scenarios and asks nothing of you. Held against a live supplier book, the same 95 produce a ranked list of the ones that can actually reach your business, a score that moves the tier a supplier is managed at, and a count of how many you would not see coming. That last number is the one worth reporting upward.

Hold the 95 against your own supplier book.
WAJD Forge supplier risk runs standalone, with or without the rest of the system.

forge@wajd.co.uk

SOURCES

National Risk Register 2026, Cabinet Office, published 14 July 2026: gov.uk/government/publications/national-risk-register-2026
National Risk Register 2025 edition, for the nine theme structure carried into 2026.
Written ministerial statement accompanying the 2026 publication, UK Parliament, 14 July 2026.