

Compliance is the floor.

Above it, every pound of RIIO-ED3 cyber spend has to earn its place in the capital plan.

Jeff Pauska, VP Product Management, IFS Copperleaf

ED3 AT A GLANCE

Price control period

1 Apr 2028 to 31 Mar 2033

Final business plans

December 2026

Draft determinations

Expected summer 2027

Image: baru mulai / Unsplash

THE ARGUMENT IN BRIEF

In 2026 the cyber threat to networked infrastructure stopped being a forecast. Frontier models now find vulnerabilities at machine speed, for attackers and defenders alike. Poorly governed agents have reached beyond their test environments, and coordinated attacks have already hijacked operational controllers across hundreds of sites in a single night. Yet most UK distribution network operators (DNOs) still weight cyber as a ring-fenced IT/OT allowance, a compliance line beside the asset plan rather than inside it.

RIIO-ED3 closes that gap. Ofgem asks for a Cyber Resilience Investment Document and a cost-benefit analysis for every material proposal, and the 2028 to 2033 period opens in the same year the NCSC expects AI-enabled attackers to exploit legacy technology across critical national infrastructure at scale.^{1,2} Our view is that cyber exposure has to become a **weighted consequence pathway on every asset decision**. It has to be priced, traded off and defensible to Ofgem in the same framework as safety, reliability and cost.

01 Six months that rewrote the threat model

The record from April to October 2026 shows the threat is here now. It reaches the same controllers, firmware and remote-access paths that sit inside every DNO's operational estate.

WHEN	SIGNAL	WHAT IT MEANS FOR A DNO
Apr 2026	Project Glasswing. Anthropic withholds Claude Mythos Preview from release after it autonomously finds zero-days in every major OS and browser. 10,000+ high/critical flaws logged; 90%+ validated. ^{3,4}	Machine-speed discovery reaches the C/C++ firmware inside RTUs, relays and gateways. Patch backlogs become a value problem.
Jun 2026	Five Eyes joint warning; NCSC at RUSI. More than 200 CNI incidents in a year, ~75% state-linked. AI-enabled exploitation of legacy technology is judged likely at scale by 2028. ^{2,5}	End-of-life OT is now classed as a strategic liability. Its replacement case is a cyber case as well as a condition case.
Jul 2026	Test agents reach production servers. OpenAI models chain a zero-day, escalate privileges and use stolen credentials to reach Hugging Face production servers, all to cheat a benchmark. ⁶	Agents pursue goals through whatever access exists. Trust boundaries and vendor remote access need a likelihood weight.
Sep to Oct 2026	Agent governance gaps beyond the US. Qwen, DeepSeek and Kimi agents lie in 84 to 88% of simulated tenders, and DeepSeek reports production agents circumventing safeguards. A Tencent-linked fleet makes 2,600+ attempts to get around Amap controls. An AI agent with server rights wipes a finished Swedish TV season, and the backup fails. ^{7,8,9}	Agents, yours and your suppliers', need the controls staff have: scoped permissions, clear accountability and a human checkpoint.
Oct 2026	French cold chain hijacked. Attackers seize Danfoss refrigeration controllers across hundreds of supermarkets overnight and drive units to 50°C. Losses run to tens of millions of euros, and some units catch fire. ¹⁰	One vendor and one controller family put hundreds of sites at risk at once. Correlated consequence is real and has to be modelled.

The pattern matters more than any single event. **Discovery has industrialised, exploitation windows have collapsed to days, and agents act through whatever access they are given.**^{2,11} Anthropic says it has withheld Mythos-class capability because “no company” yet has safeguards strong enough, and expects these capabilities to proliferate.^{3,4} For an operator patching OT on an annual outage cycle, that gap is a capital planning variable. The same capability works for defenders, which is why governed AI, with scoped access, an audit trail and a named person signing off, belongs in the answer. Ofgem’s own AI guidance asks for the same accountability and oversight.¹⁴

02 Why RIIO-ED3 turns this into a capital-planning problem

ED3 runs from 1 April 2028 to 31 March 2033. Final business plans are due in December 2026, with draft determinations expected in summer 2027.¹ Ofgem’s Business Plan Guidance requires a dedicated Cyber Resilience Investment Document alongside CBA and engineering-justification templates, and the SSMD sets “clearer expectations on climate and cyber resilience.” Government has also signalled baseline cyber requirements for all Ofgem licensees, and the Cyber Security and Resilience Bill reaches Lords report stage on 26 October 2026.^{1,12}

In ED2, cyber largely lived in its own OT and IT allowances, with separate re-opener windows tied to the CAF Enhanced Profile. That kept it auditable but **structurally isolated from the asset investment plan**. A substation refurbishment and the RTU security upgrade inside it were justified, weighted and funded on different logic. With AI-enabled attacks expected to scale against legacy CNI technology by 2028, the first year of ED3, that separation is a material risk. Cyber spend gets defended as compliance when it should be optimised as value.

A substation refurbishment and the RTU security upgrade inside it were justified, weighted and funded on different logic.

03 What the ED3 decision changes for cyber

Ofgem’s Sector Specific Methodology Decision, published on 21 May 2026, sets the cyber rules DNOs will plan against. Six of its decisions change how cyber has to be planned and defended.¹

1 One plan for IT and OT

IT and OT cyber move into a single Cyber Resilience Business Plan, aligned with NIS and the Cyber Assessment Framework. SSMD 5.225

For the capital plan: Cyber becomes one portfolio, so trade-offs between IT and OT spend have to be explicit.

2 Allowances set up front

Ofgem proposed setting cyber allowances at the outset, and keeps a use-it-or-lose-it pot capped at 20% of totex cyber allowances. SSMD 5.213, 5.227

For the capital plan: Most of the cyber plan needs a defined scope, schedule and cost before 2028.

3 No fixed re-opener window

The cyber re-opener stays, but only Ofgem can trigger it, and there is no fixed window. SSMD 5.226

For the capital plan: There is no scheduled point to repair a weak plan. In-period change has to come from reprioritising the portfolio.

4 Compliance is the floor

The CAF Enhanced Profile is a floor, rather than a ceiling. Ofgem expects DNOs to keep reducing cyber risk where that is proportionate and economically efficient. SSMD 5.228

For the capital plan: Spend above the floor is judged on value, in the same terms as any other investment.

5 Show how risks were ranked

Plans must explain how risks were prioritised, in the risk methodology section. SSMD 5.228

For the capital plan: A ranked, traceable portfolio becomes part of the submission.

6 Cyber cases read like asset cases

The Cyber Resilience Investment Document template now aligns with engineering justification papers. SSMD 5.229

For the capital plan: Cyber and asset investments are read side by side, so they need the same value logic.

04 Five shifts in how the value framework weights cyber

A value framework turns strategy into a common currency for trade-offs. To carry the 2026 threat, it has to change in five places:

LEVER	RIIO-ED2 HABIT	ED3-READY PRACTICE
1 Where cyber sits	Separate OT/IT allowance and re-opener, scored outside the asset plan	A cyber consequence pathway on every connected asset, in the same value units as safety, reliability and customer impact
2 Likelihood MOST WEIGHT	Static, assessed against the CAF annually	Exposure-driven: internet reachability, firmware support status, vendor remote access, time-to-exploit. Re-scored as intelligence changes
3 Consequence MOST WEIGHT	Single-asset, single-site	Correlated and systemic: shared vendors, controller families and managed-service providers modelled as common-mode failure
4 Legacy retirement	Justified by condition and health index (NARM)	Condition plus cyber exposure. Unsupported OT carries a priced risk premium until it is retired or isolated
5 Agentic AI	Not in scope	A governed risk category: permissions, backup integrity and human checkpoints for AI agents, your own and your suppliers'

Shifts 2 and 3 carry the most weight. Exposure-driven likelihood lets a portfolio respond the moment intelligence changes, for example when a controller family is named in a CERT advisory. Correlated consequence stops the model scoring a single vendor's fleet as hundreds of independent small risks. The French cold-chain attack showed what that fleet risk looks like in practice.¹⁰

05 Questions for DNO leadership before draft determinations

If the ED3 cyber case fails, these are the questions that would have caught it early.

DEFENDING THE PLAN

- 1 What reinforcement or asset-health work does each pound of cyber spend displace, and how would we show that trade to Ofgem in one model?
- 2 Where do our Cyber Resilience Investment Document and our engineering justification papers tell different stories about the same asset?
- 3 Who signs off the cyber weights, and what happens when the CISO and finance disagree?
- 4 How do we value a cyber consequence in the same units as safety and reliability, and where is that number weakest under challenge?
- 5 Which unsupported OT assets stay in service because they pass on condition, and what does that exposure cost us each year?

HOLDING IT THROUGH ED3

- 6 When a CERT advisory names one of our controller families, how many days pass before the portfolio is re-weighted and re-optimised?
- 7 If one vendor, controller family or managed-service provider were compromised fleet-wide, which sites fail together, and where does the plan show it?
- 8 Which AI agents (ours, our contractors', our MSPs') hold write access to operational or planning systems, and who answers for what they do?
- 9 When did we last restore an operational system from backup, and what broke?
- 10 Which baseline cyber requirements or Cyber Security and Resilience Bill duties could land mid-period, and which part of the plan pays for them?

IN THE REGULATOR'S WORDS

"[T]he CAF Enhanced Profile is a floor, rather than a ceiling ..."

Ofgem
ED3 methodology decision, para 5.228, May 2026¹

"Cyber security should be a fundamental requirement for anyone operating in our energy system."

Energy Minister and Ofgem CEO
Joint foreword, cyber regulation response, Aug 2026¹³

"...the significant potential of AI to support a safe, efficient and flexible electricity system, and the need for clear accountability, proportionate assurance and effective oversight as deployment scales."

Ofgem
Ethical AI use in the energy sector, v2, May 2026¹⁴

Ofgem is also piloting a 12-month AI technical sandbox from late autumn 2026.¹⁵

06 How IFS Copperleaf helps

IFS Copperleaf supports capital decisions for 100+ infrastructure operators in 25 countries, including GB networks. We bring two things to the ED3 cyber question: a platform that puts cyber inside the value framework, and an advisory team that has calibrated those frameworks with regulated utilities.

THE PLATFORM

IFS Copperleaf Value Framework & Portfolio

- ◆ **Cyber value measures** built from the 200+ model Value Model Library, so cyber risk is scored in the same units as every other driver of value.
- ◆ **Portfolio optimisation** that trades cyber hardening against reinforcement, flexibility and asset health under the ED3 totex envelope.
- ◆ **Scenario re-optimisation** when the threat changes: re-weight a measure and see the plan move within the hour, ready for an Ofgem-triggered re-opener.
- ◆ **Traceable calculations and audit trail** that feed EJPs, CBAs and the Cyber Resilience Investment Document.

EXPERT ADVISORY

Value Framework Advisory for ED3

- ◆ **Cyber weighting calibration:** facilitated sessions that bring the CISO, regulation, asset management and finance to one agreed set of weights.
- ◆ **Exposure-to-likelihood modelling** that turns OT inventory, vendor access and threat intelligence into defensible probabilities.
- ◆ **Systemic-consequence design** for common-mode vendor and controller-family risk.
- ◆ **Regulatory evidence packs** for draft-determination challenge, the cyber re-opener and in-period reprioritisation.

Final plans are largely written. **Weighting gets defended in the draft-determination challenge, any Ofgem-triggered cyber re-opener and every in-period reprioritisation that follows.** That is where a recalibrated framework earns its return, and where we recommend starting now.

Let's talk



Jeff Pauska
VP Product Management, IFS Copperleaf
jeff.pauska@ifs.com
Product strategy, value frameworks, ED3 platform roadmap



Nicolas Bergeron
SVP, Client Experience, IFS Copperleaf
nicolas.bergeron@ifs.com
Expert advisory, client delivery, customer success

SOURCES

- 1 Ofgem, ED3 SSMD and BPG, 2026
- 2 NCSC, UK CNI attacks statement, Jun 2026
- 3 Anthropic, Project Glasswing, Apr 2026
- 4 Help Net Security, May 2026
- 5 Five Eyes joint advisory, Jun 2026
- 6 The Hacker News, Jul 2026; PBS, Sep 2026
- 7 Reuters, China's AI agents, Sep 2026
- 8 swarmcha.se, agent fleet report, Oct 2026
- 9 Tom's Hardware / Aftonbladet, Oct 2026
- 10 CERT-FR, CERTFR-2026-ALE-012, Oct 2026
- 11 NCSC, Impact of AI on cyber threat
- 12 Osborne Clarke, Cyber outlook, Sep 2026
- 13 Govt and Ofgem, cyber regulation, Aug 2026
- 14 Ofgem, Ethical AI use guidance v2, May 2026
- 15 Ofgem, AI technical sandbox decision, 2026