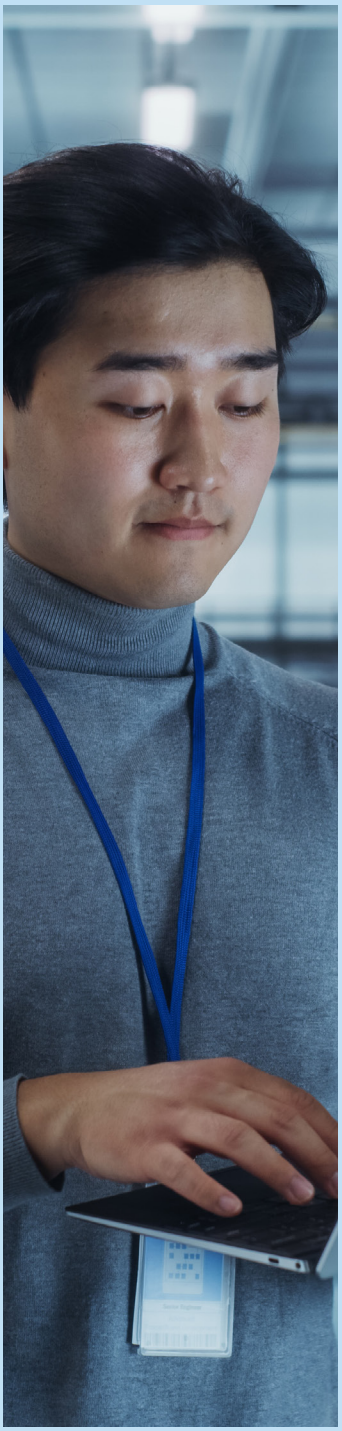
VIEW POINT



CRYPTOGRAPHY AND QUANTUM SECURITY — A POINT OF VIEW FOR UK WATER

Abstract

Post-quantum cryptography is not a cryptography problem for a water utility; it is an asset-lifecycle and capital-planning problem, and the decisions that matter most are being taken right now in AMP8 procurement[1], not in 2035.

This Point of View discards the generic enterprise migration narrative and re-states the question in the terms a water CISO actually works in: twenty-five-year plant, a regulated capital cycle, a competent authority that inspects evidence, and an operational estate in which most of the cryptography being discussed does not yet exist.

This document is an advisory Point of View. It reflects published standards and guidance current at the date of issue and does not constitute legal advice. Regulatory obligations should be confirmed with the undertaker's legal counsel and with the Drinking Water Inspectorate as competent authority.

This POV is developed for a regulated water utility to accelerate post-quantum cryptography — through AMP8, PR29 and the NCSC migration timeline. Regulatory anchors are: NIS Regulations 2018, NCSC CAF v4.0, DWI Enhanced Profile, NIST CSF 2.0, FIPS 203/204/205.

Infosys
Navigate your next

Table of Contents

Executive summary

Post-quantum cryptography has stopped being a research topic and become a capital planning topic. For a UK water and wastewater undertaker, the binding constraint is not the arrival date of a cryptanalytically relevant quantum computer (which nobody can forecast), but the length of the asset lives you are committing to today and the rigidity of the regulatory funding cycle that pays for changing them.

The National Cyber Security Centre has set out a three-phase national migration timeline: discovery and a costed migration plan by **2028**, high-priority migration complete by **2031**, and migration substantially complete by 2035. Those dates were chosen for the country as a whole. For a water company they land with unusual force, because they map almost exactly onto the asset management periods. AMP8 runs till 2030 and AMP9 already discussed till 2035. The business plan that funds AMP9 is written during 2027 and 2028 and submitted to Ofwat at PR29. If post-quantum migration is not a costed line in that submission, the undertaker enters the 2031–2035 phase with no funding envelope and no realistic path to the national end date.

This becomes the most important observation that generic post-quantum guidance does not make, **the deadline that governs a CISO within a water company is 2028, not 2035, and it is a funding deadline, which will influence a technical one.**

The second observation is that the standard industry narrative — harvest now, decrypt later, and the urgent replacement of RSA and elliptic-curve key exchange — is only partially applicable to an operational estate. Much of the deep control network in a water business carries no cryptography at all. Where that is true, there is nothing to migrate and the honest answer to a vendor pitch is that the risk is being overstated. Where cryptography does exist in the operational estate — in secure boot chains, firmware signing, engineering workstation access, vendor remote connections, telemetry over third-party carriers, and device identity — the exposure is real, and it is dominated by authenticity rather than confidentiality. A forged firmware image accepted by an outstation is a materially worse outcome for a water undertaker than a decrypted flow reading.

The third observation follows from asset life. An RTU, PLC or telemetry outstation commissioned during AMP8 will still be in service well beyond 2040. If its secure boot root of trust is anchored on an elliptic-curve key and it has no field-upgradable path to a quantum-resistant signature scheme, that decision cannot be corrected later without physically replacing the device. The cost of specifying the requirement correctly at tender is close to zero. The cost of retrofitting is a capital replacement programme. This is where the greatest value in the entire post-quantum agenda sits for a water utility, and it is available only during the current procurement window.

The five decisions to take now

#	Decision	What it means in practice	Consequence of deferral
1	Fund it at PR29	Build a costed post-quantum and cryptographic modernisation line into the AMP9 business plan during 2027–28, evidenced by a discovery exercise completed in AMP8.	No funding envelope for 2031–35; the national timeline becomes unachievable and the position is indefensible to the competent authority.
2	Fix procurement first	Insert cryptographic agility, algorithm disclosure and firmware-signing requirements into every AMP8 OT and telemetry contract still to be let.	Twenty-five years of quantum-vulnerable plant installed with your own capital, correctable only by replacement.
3	Inventory across the boundary	Extend cryptographic discovery into Purdue Levels 0–3 and the vendor estate, producing a machine-readable CBOM, not an IT-only certificate register.	A discovery exercise that looks complete, passes internal review, and omits the assets with the longest lives.
4	Prioritise authenticity	Treat code signing, firmware signing, device identity and the enterprise PKI as tier one; treat bulk confidentiality migration as tier two.	Effort spent on TLS refresh while the trust anchors that authorise change to physical process remain unaddressed.
5	Say no clearly	Adopt the NIST standardised algorithm set as the baseline and decline quantum key distribution and proprietary "quantum-proof" products.	Capital diverted to technologies that national technical authorities do not recommend for this use case.

The one-line board position

"We are treating post-quantum cryptography as an asset-lifecycle risk rather than an encryption upgrade. Our exposure is concentrated in long-lived operational plant and in the trust anchors that authorise change to it. We will complete discovery and a costed plan within AMP8 so that the migration itself is funded through PR29, and in the meantime we will stop the problem growing by fixing what we specify in AMP8 contracts."

Why a water utility is not a generic enterprise

Almost all published post-quantum migration guidance is written for an estate of servers, applications, browsers and cloud services with a three-to-seven year refresh cycle. In that world, migration is a scheduling exercise: the crypto changes when the software changes, and the software changes often. A water undertaker does not live in that world, and applying the generic model produces a plan that is simultaneously too urgent about the wrong things and far too relaxed about the right ones.

Four structural characteristics make the sector different, and each of them changes the answer.

Asset lives measured in decades

The refresh cycle of an enterprise application is shorter than the commissioning period of a treatment works. Programmable controllers, telemetry outstations, instrumentation, panel hardware and safety systems are specified, installed and then left in service for as long as they perform their function safely. The planning assumption a CISO should adopt is that anything installed on a site during AMP8 will still be there in the mid-2040s, and that the distribution and sewerage network assets it monitors have design lives measured in the better part of a century.

The consequence is that the migration question inverts. For enterprise IT the question is "how quickly can we replace the cryptography that is already deployed?" For operational technology the question is "what cryptography are we about to deploy, and will it still be defensible when this asset is halfway through its life?" The second question has a much cheaper answer and a much shorter window in which to answer it.

Capital is allocated by a regulator, not by the business

Expenditure is set through the price review process for a five-year period. Within a period there is limited scope to introduce a new multi-year programme that was not in the plan; between periods there is a hard submission date. A cyber programme that cannot articulate its cost in the business plan does not get funded, and a cyber programme that cannot evidence why the cost is necessary does not survive the regulator's challenge. This is why discovery has a value in this sector that it does not have elsewhere: discovery is not just a technical prerequisite, it is the evidence base for the funding case.

The competent authority inspects evidence

The Drinking Water Inspectorate enforces the NIS Regulations for drinking water in England and Wales and has been moving the sector toward the Enhanced Profile of the Cyber Assessment Framework, with verification rather than self-assertion. The practical implications for post-quantum work is that an assertion of intent is worth very little. A dated cryptographic inventory, a documented prioritisation method, a supplier engagement record and a costed plan are worth a great deal, and they are also exactly what the NCSC asks for in the first migration phase. The regulatory and the technical requirement point at the same artefacts.

Safety and availability outrank confidentiality

In a bank, the worst cryptographic failure is usually disclosure. In a water business, the worst cryptographic failure is an unauthorised or spoofed instruction that changes the physical process — a dosing setpoint, a pump start, a valve position, a level alarm suppressed. That reorders the entire priority list. It is also the reason a migration that introduces instability into control communications is not an acceptable trade: a post-quantum handshake that adds latency or fragmentation to a marginal radio telemetry link can cause a genuine operational incident, whereas the risk it mitigates is speculative and years away.

Assessment take away:

Much of the post-quantum material being marketed into critical national infrastructure is enterprise IT guidance with the word "OT" inserted. It recommends TLS inventory sweeps, certificate lifecycle tooling and hybrid key exchange across the estate. Applied literally in a water business, that produces a large bill, a report that stops at the IDMZ, and no reduction in the risk that actually matters. The test to apply to any post-quantum proposal is simple: does it change what we specify for plant we are about to install, and does it protect the trust anchors that authorise change to the process? If not, it is deferrable.

Key Obligations

It is worth being precise about the difference between legal obligation, regulatory expectation and technical guidance, because the three are routinely conflated in vendor material and the distinction determines how the programme should be argued internally.

Instrument	Status	What it requires that is relevant here	Implication for post-quantum work
NIS Regulations 2018	Binding law	Operators of essential services must take appropriate and proportionate technical and organisational measures to manage risk to network and information systems, and report incidents to the competent authority.	Foreseeable cryptographic obsolescence in long-lived assets is a risk you are on notice of. Proportionality is judged against published guidance.
DWI as competent authority	Enforcement	Assesses drinking water operators against the CAF, sets the applicable profile, conducts verification, and holds enforcement powers under the Water Industry Act.	Your post-quantum position will be examined as evidence within a CAF assessment, not as a separate exercise.
NCSC CAF v4.0	Assessment framework	Outcome-based contributing outcomes across governance, risk, supply chain, identity, data and system security. Released August 2025.	Provides the vocabulary for evidencing the programme. See section CAF v4.0 alignment for the mapping.
Enhanced Profile (eCAF)	Sector expectation	A curated, more demanding subset of outcomes applied to critical systems, with an expectation of attainment around 2028 in the water sector.	The 2028 expectation coincides with the NCSC discovery milestone and with PR29. Treat as one deadline.
Cyber Security and Resilience Bill	In passage	Introduced November 2025; passed to the House of Lords in June 2026, progressing toward Royal Assent. Extends NIS scope to managed service providers, data centres and designated critical suppliers, and strengthens regulator powers and reporting timelines.	Expands the population of suppliers you can and should hold to cryptographic requirements. Confirm current status before publication.
NCSC PQC timelines	Guidance	Discovery and plan by 2028; high-priority migration by 2031; migration complete by 2035.	Not directly binding, but it is the benchmark a regulator will reach for when testing proportionality.
NIST FIPS 203/204/205	Standards	ML-KEM for key establishment, ML-DSA and SLH-DSA for digital signatures, finalised August 2024.	The algorithm baseline. NCSC endorses the NIST set for UK use.
NIST SP 800-208	Standards	Stateful hash-based signatures (LMS, XMSS) approved for firmware and software signing.	The practical answer for constrained device secure boot today. See section The authenticity problem.

A distinction worth defending internally -

The 2035 date is not a statutory deadline for a water undertaker. Presenting it as one damages credibility, and a well-briefed finance director will find the flaw. The defensible argument is different and stronger: NIS-R requires proportionate measures against foreseeable risk; the NCSC has published what proportionate looks like and when; the competent authority is moving to evidence-based verification; and our asset lives mean deferral removes options rather than preserving them. That argument survives challenge. "It is mandatory by 2035" does not.

The funding window: AMP8, PR29 and AMP9

This section contains the practical core of the Point of View. Everything technical in the remainder of the document is downstream of a scheduling fact.

The national migration timeline and the regulated capital cycle are almost perfectly interleaved, and not by design. AMP8 began in April 2025 and runs to March 2030. AMP9 runs from 2030 to 2035. The business plan for AMP9 is developed through 2027 and 2028 and submitted at the PR29 price review. The NCSC expects discovery and a migration plan to be complete by 2028, high-priority migration between 2028 and 2031, and completion between 2031 and 2035.

Overlay those two and the conclusion is unavoidable. The bulk of the migration effort — the part that costs real money, because it involves plant, PKI platforms, HSM estates, application remediation and supplier-delivered upgrades — falls in AMP9. AMP9 is funded by a plan written in AMP8. Therefore, the discovery exercise is not merely the first technical phase; it is the evidence pack for the funding submission, and it has to be finished early enough to be costed and challenged internally before the plan is locked. Working backwards from a 2028 submission, discovery needs to be substantially complete during 2027, which means it needs to be scoped, resourced and started in the current financial year.

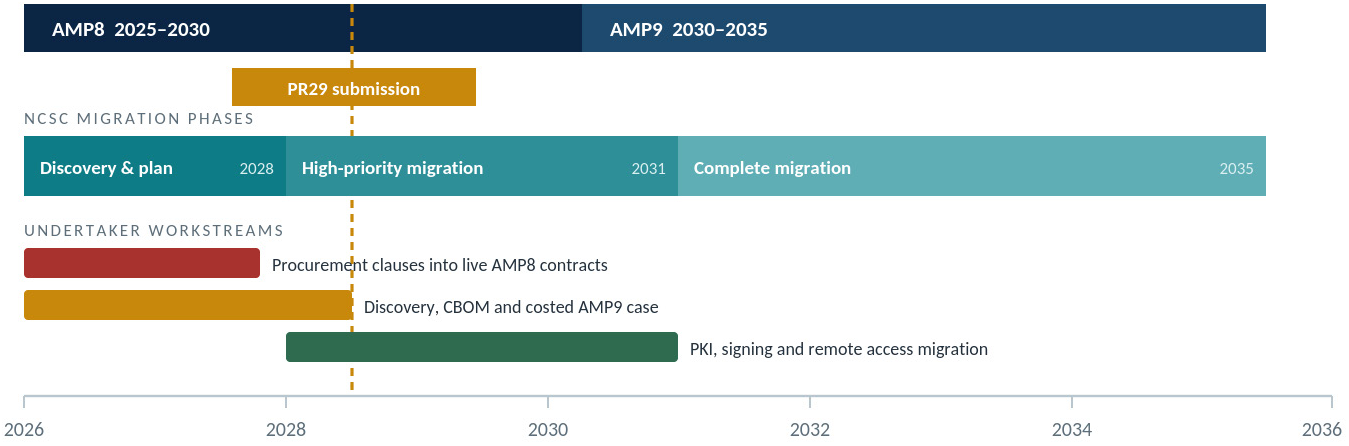


Figure 1 — The NCSC migration phases mapped against the regulated capital cycle. The PR29 submission window is the binding constraint: work that is not evidenced by then cannot be funded in AMP9.

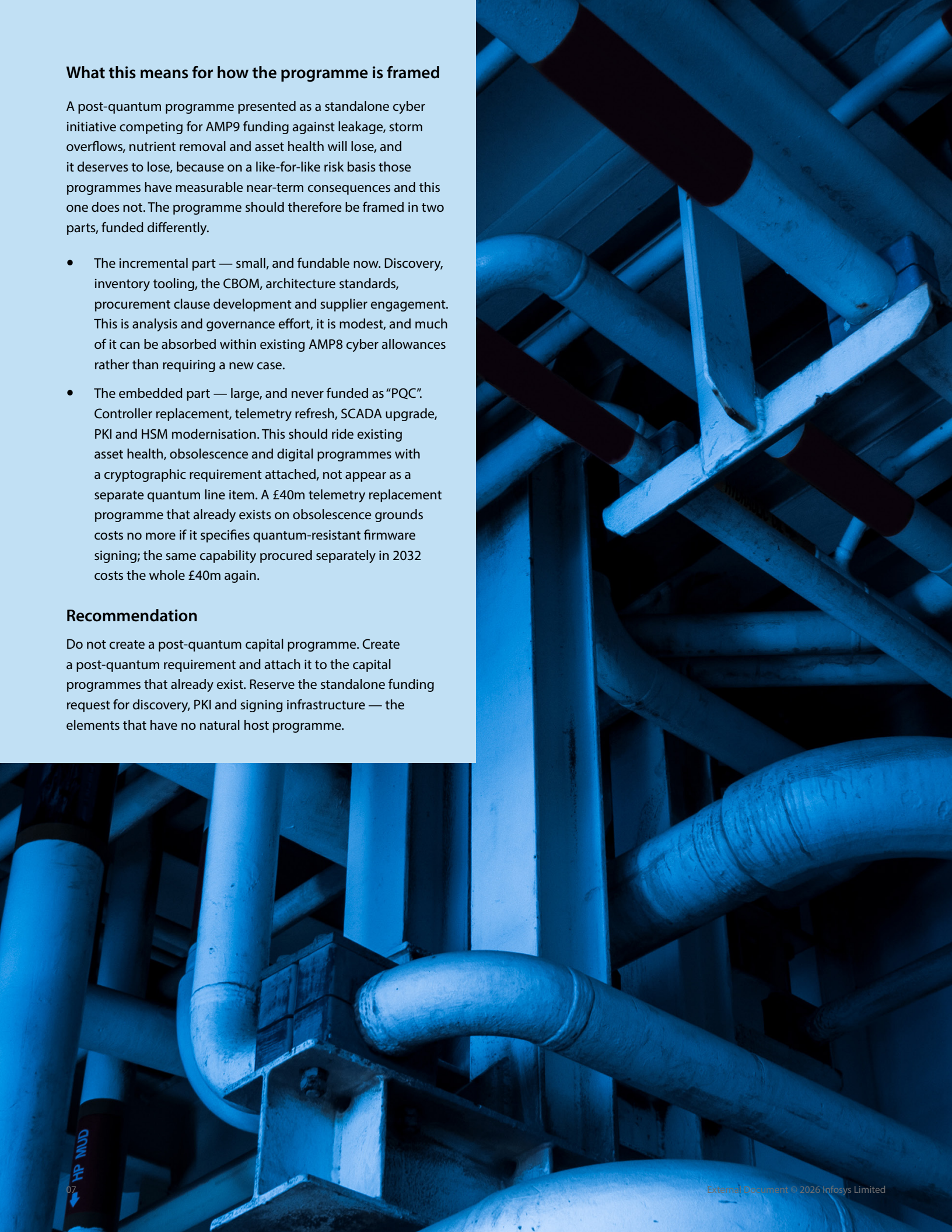
What this means for how the programme is framed

A post-quantum programme presented as a standalone cyber initiative competing for AMP9 funding against leakage, storm overflows, nutrient removal and asset health will lose, and it deserves to lose, because on a like-for-like risk basis those programmes have measurable near-term consequences and this one does not. The programme should therefore be framed in two parts, funded differently.

- The incremental part — small, and fundable now. Discovery, inventory tooling, the CBOM, architecture standards, procurement clause development and supplier engagement. This is analysis and governance effort, it is modest, and much of it can be absorbed within existing AMP8 cyber allowances rather than requiring a new case.
- The embedded part — large, and never funded as "PQC". Controller replacement, telemetry refresh, SCADA upgrade, PKI and HSM modernisation. This should ride existing asset health, obsolescence and digital programmes with a cryptographic requirement attached, not appear as a separate quantum line item. A £40m telemetry replacement programme that already exists on obsolescence grounds costs no more if it specifies quantum-resistant firmware signing; the same capability procured separately in 2032 costs the whole £40m again.

Recommendation

Do not create a post-quantum capital programme. Create a post-quantum requirement and attach it to the capital programmes that already exist. Reserve the standalone funding request for discovery, PKI and signing infrastructure — the elements that have no natural host programme.



Understanding the Exposure Landscape

The following assessment is deliberately unflattering to parts of the standard narrative. It separates the estate by where cryptography genuinely exists, how long the protected property needs to survive, and whether the asset can be changed in the field.

Asset class	Cryptography typically present	Quantum exposure	Field upgradable?	Priority	Comment
Firmware & secure boot on controllers, RTUs, instruments	Vendor signing keys, usually ECDSA or RSA; root of trust often in silicon	High — signature forgery	Rarely; often not at all	Tier 1	The defining problem. Cannot be corrected after installation. Must be fixed at specification.
Code signing & software distribution	RSA/ECDSA signing, internal and vendor	High — forged trusted update	Yes, with effort	Tier 1	Compromise here propagates to every asset that trusts the chain.
Enterprise and OT PKI, HSMs, certificate services	RSA/ECC hierarchies, HSM-protected roots	High — trust anchor	Yes, but slow and disruptive	Tier 1	Long lead time. HSM firmware support for PQC must be confirmed with the vendor, not assumed.
Remote access: vendor, OEM and out-of-hours engineering	TLS, IPsec, SSH; classical key exchange	High — harvested session, forged identity	Yes	Tier 1	Highest-consequence pathway into the process. Also the easiest to migrate.
Network and hydraulic models, asset schematics, site drawings	Encryption at rest and in transit for shared copies	High — very long sensitivity life	n/a — data	Tier 1	See section Harvest now, decrypt later. This is the genuine harvest-now-decrypt-later case in this sector.
IT/OT boundary, IDMZ brokers, historian replication	TLS, mutual authentication, VPN	Medium	Yes	Tier 2	Migrate on ordinary refresh with hybrid key exchange where supported.
Telemetry over third-party carriers, private APN, licensed radio	Variable; often carrier-level only, sometimes none	Medium	Sometimes	Tier 2	Constrained links. Do not mandate hybrid without testing fragmentation and latency impact.
Customer, billing, HR and legal records	TLS, database and backup encryption	Medium	Yes	Tier 2	Retention periods make some of this long-lived. Confirm actual periods with Legal.
Cloud, SaaS, corporate identity platforms	Provider-managed TLS and key management	Medium	Provider-dependent	Tier 2	Largely a supplier assurance question. Ask for roadmaps; do not build it yourself.
Level 0–1 process communications: 4–20 mA, HART, Modbus, unauthenticated DNP3, Profibus	None	None	n/a	Not applicable	There is no cryptography to migrate. The security problem here is real but it is segmentation and authentication, not quantum.
Live process telemetry values in transit	Where present, session encryption	Low	n/a	Low	A flow or level reading has almost no confidentiality value once it is a day old. Resist the harvest-now framing here.

Table 1 — Exposure assessment. Priorities reflect consequence and irreversibility, not the volume of cryptography present.

Assessment take away:

Two rows of that table deserve emphasis because they are usually reported in the opposite direction. First, the deep control network is not a post-quantum problem at all, because it has no cryptography to break; any proposal that spends money there under a quantum banner is solving a different problem and should be funded on its own merits as segmentation or protocol authentication work. Second, the highest-value item on the list is not encryption of anything — it is the signing key that decides which firmware an outstation will accept. That row rarely appears in a standard cryptographic inventory, because standard inventory tooling discovers certificates and TLS endpoints, and a secure boot root of trust is neither.

Harvest now, decrypt later

The harvest-now-decrypt-later argument holds that an adversary capable of intercepting encrypted traffic today can store it and decrypt it once a sufficiently capable quantum computer exists, which means the effective protection period of anything encrypted today ends when the mathematics fails rather than when the retention policy says it does. The argument is sound. Its force depends entirely on how long the intercepted material stays valuable, and that is where a water-specific reading diverges sharply from the generic pitch.

For most operational data the answer is: not long. A pump status, a chlorine residual reading or a level alarm from 2026 has essentially no confidentiality value in 2036. Presenting harvested telemetry as a strategic risk to a water board is an argument that will not survive a moment's reflection, and making it costs the CISO credibility on the points that do matter.

There are, however, four categories in a water business where the sensitivity life is genuinely long — in two cases longer than in almost any other sector.

Category	Sensitivity horizon	Why it matters
Network models, hydraulic models, asset schematics, site layouts, isolation and valve plans	Decades — effectively the life of the buried asset	A distribution or sewerage network laid today will largely still be in the ground in the 2090s. A hydraulic model disclosing single points of failure, critical mains, pressure-managed zones and isolation strategy remains an operationally useful targeting document for as long as the network exists. This is the strongest harvest-now case in the sector and it is very rarely the one that is made.
Site security arrangements, CNI designations, resilience plans, SEMD material	Decades	Physical site arrangements change slowly. Documentation describing them retains value for as long as the arrangements persist.
Customer, employee and legal records	Years to decades, driven by statutory and limitation periods	Personal data carries disclosure and regulatory consequence long after the commercial relationship ends. Actual retention periods should be confirmed with Legal rather than assumed.
Long-lived credentials and key material	Life of the device or certificate hierarchy	A device identity or root key harvested today remains useful for as long as the trust hierarchy stands. This overlaps with the authenticity problem in section 7 and is arguably the more urgent framing.

Table 2 - Four Water Business Categories with Long Asset Sensitivity Lifecycles

Recommendation

Run a targeted long-lived-data classification rather than an estate-wide one. Identify where hydraulic and network models, site and resilience documentation, and regulated personal records are stored, transmitted and shared — particularly with consultants, framework contractors and design partners, where these files most often leave the perimeter. Protect those flows first. That exercise is small, cheap, defensible to a regulator, and it targets the only category in which the harvest-now argument is genuinely strong for a water undertaker.

The authenticity problem

If a single technical section of this document justifies its length, it is this one. The public debate about post-quantum cryptography is dominated by encryption, because the harvest-now argument is vivid and easy to explain. For a water undertaker the more serious exposure is the reverse: not the reading of protected data, but the forging of trusted instructions and trusted software.

Digital signatures underpin the mechanisms by which change is authorised in an operational estate. Firmware images are signed by the vendor and verified by the device. Engineering software and controller logic are signed and verified before deployment. Device identities are certificates issued from a hierarchy rooted in a signing key. Update servers, patch repositories and configuration management systems all rest on signature verification somewhere. When the signature algorithm fails, the guarantee that fails is not privacy — it is the guarantee that the thing you are installing came from who you think it came from.

The specific hazard for this sector is the interaction of that with asset life and field upgradability. Consider a telemetry outstation specified in 2027 under an AMP8 framework, installed in 2029, with a secure boot root of trust burned into hardware and verifying vendor firmware with an elliptic-curve signature. It is expected to serve until at least the mid-2040s. There is no software update that can change a hardware root of trust. If a quantum-capable adversary emerges within that window, every one of those outstations will accept a forged firmware image, and the only remediation is to physically visit and replace several thousand devices distributed across the operating region.

The decision you are taking without realising it:

Every OT tender issued between now and 2030 either does or does not require a quantum-resistant path for firmware verification. If the requirement is absent, the default answer is no, and the undertaker has committed to a twenty-year exposure at the moment of contract award. This decision is currently being taken by procurement and engineering teams who have not been asked the question.

What to require, and what is realistic

The instinctive answer — require ML-DSA everywhere — is not deliverable in 2026 across constrained hardware and specifying it as a hard gate will simply result in tenders being returned non-compliant or, worse, compliant on paper. A graduated requirement works better.

Signing use case	Baseline to require	Notes and constraints
Firmware and secure boot, constrained devices	LMS or XMSS per NIST SP 800-208, or ML-DSA where the platform supports it	Stateful hash-based schemes are approved specifically for firmware and software signing, rest on conservative hash assumptions and have relatively small verification cost, which suits constrained verifiers. The critical caveat is that they are stateful: reusing a one-time key index catastrophically breaks security, so the signing side demands rigorous, auditable state management. That burden sits with the vendor, and vendor state management practice is a legitimate assurance question to ask at tender.
Firmware and software signing, capable platforms	ML-DSA (FIPS 204), with SLH-DSA as a diversity option	Stateless and operationally simpler. Larger signatures and keys than ECDSA; verify the impact on image formats, update channels and any size-constrained transport.
Enterprise code signing and internal software supply chain	ML-DSA, dual-signed with the existing classical scheme during transition	Dual signing preserves compatibility with verifiers that cannot yet parse post-quantum signatures. Confirm that verifiers ignore rather than reject unknown signature blocks.
Device identity and certificate hierarchies	Migration plan with dates; hybrid or dual hierarchy during transition	Long lead time. Confirm HSM firmware and CA product support explicitly; do not accept a marketing statement of PQC readiness without a version number and a date.
Where none of the above is achievable	Contractual commitment to a defined upgrade path, with dates and a remedy	If the hardware genuinely cannot support a quantum-resistant root of trust, that is an accepted risk with a compensating control and an asset replacement date — recorded formally, not discovered in 2033.

The compensating position, where a device cannot be made quantum-resistant, is unchanged from good OT practice generally: strong network segmentation, tightly controlled and monitored update paths, out-of-band verification of firmware provenance, and physical control of engineering access. These controls do not solve the cryptographic problem, but they materially reduce the exploitability of it, and they are already required by the CAF.

The algorithm baseline

The standards position is settled enough that there is no reason for a water undertaker to hold an internal debate about algorithm selection. NIST finalised the first post-quantum standards in August 2024 and the NCSC endorses them for UK use. The correct posture is to adopt the mainstream set, avoid premature diversification, and preserve the ability to change later.

Purpose	Standard	Status	Guidance for this estate
Key establishment	ML-KEM — FIPS 203	Adopt	Default for TLS, IPsec, SSH and any new key exchange. Use in hybrid combination with the existing classical scheme wherever the protocol and both endpoints support it. Select the parameter set by data sensitivity rather than defaulting to the largest.
General signatures	ML-DSA — FIPS 204	Adopt	Default general-purpose signature scheme for PKI, code signing and capable device platforms.
Signature diversity	SLH-DSA — FIPS 205	Reserve	Hash-based, different mathematical assumptions to ML-DSA. Worth holding as a fallback for the highest-assurance trust anchors. Larger signatures; check size tolerance before committing.
Firmware and software signing	LMS / XMSS — SP 800-208	Adopt for OT	Approved specifically for this use case and generally the most practical option for constrained verifiers today. Stateful — see the caveat in section The authenticity problem.
Symmetric encryption	AES-256	Sufficient	No migration required. Where AES-128 is in use for long-lived data, move to 256-bit on ordinary refresh. This is a low-cost, low-risk win worth taking early.
Hashing	SHA-256 / SHA-384 / SHA-3	Sufficient	No migration required. Retire SHA-1 wherever it survives, which in an OT estate is more often than most inventories suggest.
Backup key encapsulation	HQC	Monitor	Selected by NIST as a backup mechanism based on different assumptions to ML-KEM. Design for the possibility of substitution; do not deploy ahead of the mainstream.
Compact signatures	FN-DSA and additional signature candidates	Monitor	Relevant where signature size is a hard constraint, which occurs in some telemetry and embedded contexts. Track but do not plan around it yet.

Where hybrid is right, and where it is not

Hybrid key exchange — combining a classical and a post-quantum mechanism so that the connection is secure if either holds — is the correct default for internet-facing services, corporate TLS, remote access and the IT/OT boundary. It is not automatically correct on constrained links. Post-quantum key material is substantially larger than elliptic-curve material, and on a narrowband radio or metered cellular telemetry link that can mean additional round trips, fragmentation, retransmission under marginal signal, or simply a handshake that no longer completes within the timeout. Mandating hybrid across the telemetry estate without link-level testing is a realistic way to cause an availability incident in pursuit of a distant risk. Test first; exempt with documented justification where necessary.

What not to buy

A CISO in this sector will be approached by vendors positioning quantum products against critical national infrastructure, and the funding cycle makes it tempting to bundle something visible into a business case. Three categories deserve a clear internal position so that the answer can be given quickly and consistently.

Quantum key distribution

QKD uses quantum physical properties to establish keys over dedicated optical links. It is genuine science and it is not a fit for a water undertaker. It requires special-purpose hardware and dedicated fibre, does not authenticate endpoints on its own, cannot be delivered in software, and does not address the signature and authenticity problems that dominate this estate. The US National Security Agency does not recommend it for national security systems and considers mathematically-based quantum-resistant cryptography the more cost-effective and maintainable path. The NCSC has taken a comparably cautious public position. For a geographically dispersed estate of thousands of sites connected by radio and cellular telemetry, QKD is not merely unnecessary — it is architecturally impossible.

Proprietary "quantum-proof" algorithms

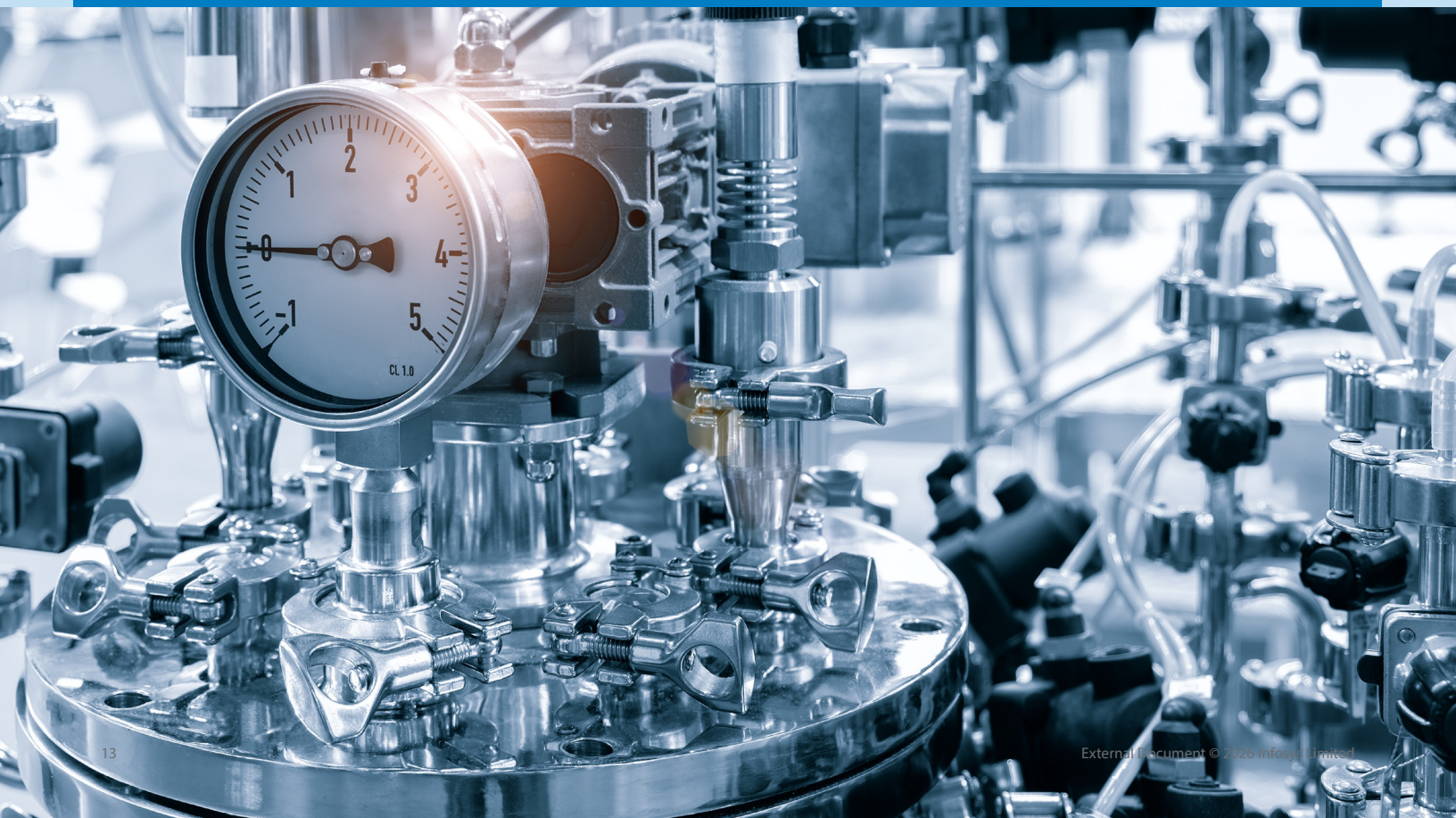
Any product claiming quantum resistance through a proprietary or unpublished algorithm should be declined without further evaluation. Cryptographic confidence comes from sustained public analysis. A scheme that has not been through that process has no assurance basis regardless of the strength of the marketing claim, and adopting one would be difficult to defend to a competent authority.

Quantum random number generators sold as post-quantum migration

Hardware entropy sources are a legitimate component and may be worth having on their merits. They are not post-quantum cryptography, they do not reduce exposure to quantum cryptanalysis of public-key algorithms, and they should not be counted as migration progress.

Recommendation

Publish a one-page internal position on quantum procurement, signed by the CISO, stating that the undertaker adopts the NIST standardised algorithm set and will not procure QKD or proprietary quantum-resistant cryptography during this period. It saves a great deal of evaluation effort and it gives engineering and procurement colleagues a defensible answer to give without escalating.



Crypto-agility, and where it does not apply

Crypto-agility — the ability to change cryptographic algorithms without redesigning the system that uses them — is now treated by NIST as a first-class operational capability rather than a design aspiration. It is the right principle for the IT estate and for new software. Applied to the operational estate without qualification it is a category error, and one worth naming because it appears in almost every post-quantum policy document written for critical infrastructure.

A hardware root of trust is not agile and cannot be made agile. A controller with cryptographic primitives implemented in silicon is not agile. A device with no field firmware update path is not agile, and in some safety-related contexts it should not be, because a remotely updatable safety controller is a different and larger risk. Writing "all systems shall be crypto-agile" into a standard produces one of two outcomes: an unenforceable requirement that everyone quietly ignores, or a stream of exceptions that consumes the architecture function's time and teaches the organisation that the standard is negotiable.

The operational equivalent of agility is different, and it should be stated in its own terms.

Estate	Agility mechanism	What to require
Corporate IT, cloud, new applications	Genuine crypto-agility	Abstraction over cryptographic providers, no hard-coded algorithm or certificate assumptions, negotiated algorithms where the protocol allows, configuration rather than code changes.
Level 3–3.5: SCADA servers, historians, IDMZ, engineering workstations	Partial agility via platform refresh	Vendor-supported algorithm configuration, current supported software versions, documented upgrade path with dates.
Level 1–2: controllers, RTUs, outstations, instruments	Procurement-time selection plus planned replacement	You get one decision, taken at tender. Require the strongest available quantum-resistant verification path, a documented firmware update mechanism, and an explicit statement of what cannot be changed after installation. Record that statement in the asset register alongside the replacement date.
Level 0: instrumentation and final elements	Not applicable	Manage by segmentation and physical control. Do not write cryptographic requirements that cannot be met.

Assessment take away:

A standard that mandates agility uniformly across an OT estate will be ignored by the people closest to the plant, and rightly so. A standard that says clearly where agility is required, where the equivalent control is procurement-time selection, and where the honest answer is segmentation and a replacement date, will be followed. The credibility of the whole cryptographic control set depends on getting this distinction right, because it is the point at which engineering colleagues decide whether the policy was written by someone who understands the estate.

Cryptographic inventory and the CBOM

Discovery is the first phase of the national timeline, the evidence base for the funding submission, and the artefact a competent authority will ask to see. It is also the phase most commonly declared complete when it is not.

The characteristic failure is well understood and easy to predict. Commercial cryptographic discovery tooling is built for enterprise networks. It scans hosts, terminates or observes TLS, enumerates certificates, reads key stores and produces a good picture of the corporate estate. It cannot safely scan a control network, it does not understand industrial protocols, it will not find a signing key inside a vendor's build pipeline, and it has no visibility of what algorithm a controller uses to verify its own firmware. The result is a report that is accurate, professionally produced, and silent on precisely the assets with the longest lives and least remediability.

What a defensible inventory contains

Layer	How it is discovered	What must be recorded
Corporate IT and cloud	Automated discovery, certificate management platforms, code repository and build pipeline scanning	Algorithm, key length, certificate expiry, owner, protocol, data classification, retention profile
OT Levels 3–3.5	Passive monitoring from the existing OT visibility platform, plus configuration review	As above, plus vendor, product version, supported algorithm set, upgrade path
OT Levels 1–2	Vendor questionnaire and documentation review — not scanning	Secure boot mechanism, firmware signing algorithm, whether the root of trust is field-changeable, device identity scheme, asset replacement date
Suppliers and managed services	Structured supplier questionnaire and contract review	Product-level algorithm support, roadmap dates by product family, hidden dependencies in firmware, SDKs and appliances
Data	Records and information management, working with Legal	Confidentiality and authenticity lifetime by category, storage and transmission paths, third parties holding copies

Recording it as a CBOM

The inventory should be produced as a cryptographic bill of materials in a machine-readable, standards-based format rather than as a spreadsheet. CycloneDX supports cryptographic asset inventory and is published as ECMA-424; using it means the inventory can be generated from build pipelines, exchanged with suppliers, versioned, and diffed over time rather than re-created annually by hand.

The practical argument for this is not elegance. An inventory that must be manually rebuilt will be rebuilt once, for the funding submission, and will then decay. An inventory that is generated and version-controlled becomes a live control that can evidence progress to a regulator every year between now and 2035, which is precisely the reporting horizon the programme has to survive.

Recommendation

Treat the CBOM as an extension of the existing software bill of materials capability and the asset register, not as a new tool purchase. Require suppliers to provide cryptographic asset information in CycloneDX format as part of the same clause that requires an SBOM. For the Level 1–2 estate, accept that the first iteration will be built from vendor documentation and questionnaires, and record the confidence level explicitly — a documented low-confidence entry is a finding; a blank row is a gap nobody will notice.

Supply chain: the AMP8 procurement window

Almost nothing in the operational estate is built by the undertaker. Controllers, telemetry, instrumentation, SCADA platforms, MEICA packages and increasingly the design and delivery of whole schemes come through frameworks and delivery partners. The cryptography that will be in the ground in 2045 is therefore being chosen by suppliers, under contracts being awarded now, against specifications that in most cases say nothing about it.

This is the cheapest control available in the entire programme and it has a closing window. A requirement inserted into a specification before award costs specification effort. The same capability retrofitted after installation costs a capital replacement.

Clauses to insert into OT and telemetry procurement

- **Cryptographic disclosure.** The supplier shall declare all cryptographic algorithms, key lengths, protocols and certificate hierarchies used in or by the supplied product, including those used for firmware verification, secure boot, device identity and any embedded third-party components, in CycloneDX format.
- **Firmware verification path.** The supplier shall state whether the product supports, or has a committed roadmap to support, quantum-resistant firmware signature verification per NIST SP 800-208 or FIPS 204, with a version and a date; and shall state explicitly whether the root of trust can be changed after installation.
- **Algorithm change.** The supplier shall state the mechanism and lead time by which cryptographic algorithms in the product can be changed during its service life, and the conditions under which this is not possible.
- **Roadmap commitment.** The supplier shall provide a post-quantum roadmap for each product family supplied, updated annually for the duration of the contract.
- **Support horizon.** The supplier shall confirm the date to which security updates, including cryptographic updates, will be provided, and the process at end of support.
- **Notification.** The supplier shall notify the undertaker where a cryptographic component in a supplied product is deprecated, withdrawn or found deficient.

Expect a difficult first round -

Many OT suppliers will not be able to answer these questions well in 2026, and some will not be able to answer them at all. That is not a reason to drop the clauses. The answers themselves are the discovery exercise for the supplier-delivered portion of the estate, an inability to answer is a material finding for the risk register, and asking the question consistently across a framework is the single most effective way a large purchaser moves a supply base. The undertakers that ask in 2026 will be buying from a better-prepared market in 2029; those that wait will be buying whatever the market happens to offer.

The Cyber Security and Resilience Bill, once in force, will extend regulatory scope over managed service providers and designated critical suppliers, which strengthens the position from which these requirements can be set. The requirements should not wait for it.

Roadmap 2026–2035

The following roadmap aligns the national migration phases to the capital cycle. The dates are programme milestones, not predictions about when a quantum computer will exist; their purpose is to sequence decisions while that uncertainty persists.

Period	Regulatory context	Objectives	Evidence produced
2026 Now	AMP8 delivery; CAF v4.0 assessment cycle	Establish governance under joint CISO and CIO sponsorship. Publish the cryptographic position and the quantum procurement position. Insert clauses into live and forthcoming AMP8 contracts. Scope and mobilise discovery. Retire SHA-1 and AES-128 for long-lived data where found.	Terms of reference; two-page internal position papers; amended specification templates; discovery plan; risk register entries
2027	PR29 plan development	Complete discovery across IT, OT and suppliers. Produce first CBOM. Classify long-lived data with Legal. Complete the tier-one prioritisation. Confirm PKI and HSM vendor roadmaps. Cost the AMP9 requirement.	CBOM v1; prioritised asset list; supplier readiness assessment; costed AMP9 investment case
2028	PR29 submission; NCSC phase-one milestone; eCAF expectation	Submit the funded plan. Begin tier-one migration: remote access, IT/OT boundary, code signing. Pilot post-quantum signing in a controlled OT context. Complete corporate hybrid TLS rollout for internet-facing services.	Submitted business plan; pilot results with performance data; migration plan v2; CAF evidence pack
2029–2030	End of AMP8	Migrate enterprise PKI and code signing infrastructure. Complete remote access migration. Embed cryptographic requirements as standard in all AMP9 framework awards. Confirm AMP9 delivery sequencing.	PKI migration record; framework specifications; updated CBOM
2031	NCSC phase-two milestone	Tier-one migration complete. High-priority OT assets migrated or on a committed replacement schedule. Refresh the plan against standards developments including backup algorithms.	Phase-two completion statement; residual risk register with named acceptances
2032–2035	AMP9 delivery; NCSC end date	Complete tier-two migration through asset refresh. Retire classical-only trust anchors. Manage the long tail of non-upgradable plant through documented acceptance and scheduled replacement.	Annual CBOM; closure evidence; accepted-risk schedule with replacement dates

On the long tail -

A water undertaker will not have a fully quantum-resistant estate in 2035, and no serious plan should claim otherwise. There will be plant installed in the 2020s that is still operating, cannot be upgraded, and is not yet due for replacement. The defensible position is not completion; it is a small, known, documented population of accepted exceptions, each with a compensating control and a replacement date, reviewed annually. That is a position a competent authority can accept. A claim of full completion that does not survive inspection is a considerably worse outcome.

The Initial 12-Month Journey

The following is deliberately short. It is the set of actions that must complete before the funding case can be written, and it is achievable within existing AMP8 cyber resource.

#	Action	What good looks like	Owner	Why it is on this list
1	Establish joint governance	Named CISO and CIO sponsors, engineering and asset management represented, decision rights defined, monthly cadence, reporting line into the existing cyber programme rather than a new forum	CISO and CIO	Fragmented ownership is the most common failure mode; without asset management in the room the AMP linkage will not be made
2	Amend procurement specifications	Cryptographic disclosure, firmware verification and roadmap clauses in every OT, telemetry and MEICA specification template; existing framework suppliers formally notified	Procurement with Security Architecture	Closing window; the cheapest control in the programme
3	Scope and start discovery	Method agreed for IT, OT and supplier layers; OT approach explicitly passive; confidence levels recorded; output in CycloneDX	Security Architecture with OT Engineering	Long lead time and it is the evidence base for PR29
4	Classify long-lived data	Hydraulic and network models, site and resilience documentation, and regulated personal records identified with storage, transmission and third-party sharing paths mapped	Legal, Records, Data	The only genuinely strong harvest-now case in this sector
5	Map the signing estate	Every signing key, its holder, its algorithm and the population that trusts it — internal and vendor	PKI and Platform Engineering	Standard discovery tooling will not find this; it is tier one
6	Confirm PKI and HSM roadmaps	Written vendor statements with product versions and dates, not marketing claims of readiness	PKI and Platform Engineering	Longest technical lead time in the programme
7	Publish the two positions	Cryptographic standards position and quantum procurement position, each one to two pages, CISO signed	CISO	Stops uninformed decisions and vendor-led evaluations immediately
8	Baseline new cryptography	All new asymmetric use in the IT estate is post-quantum ready or crypto-agile; formal exception process for anything else	Security Architecture	Stops the problem growing while discovery runs
9	Pilot on a real link	Hybrid key exchange tested on a representative constrained telemetry link with measured latency, fragmentation and failure behaviour	OT Engineering	Turns the section-The algorithm baseline caution into evidence and prevents a mandated rollout causing an incident
10	Open the funding conversation	Post-quantum requirement recognised in AMP9 planning assumptions; a named finance contact	CISO with Regulation and Finance	The PR29 window closes earlier than most technical teams expect

Aligning to CAF v4.0

Post-quantum work should be evidenced within the existing CAF assessment rather than presented separately. The mapping below indicates where the artefacts produced by this programme contribute. Objective and outcome references should be confirmed against the current published CAF text and the profile set by the competent authority before use in a submission.

CAF area	Relevance to post-quantum work	Evidence this programme produces
A2 — Risk management	Cryptographic obsolescence as an identified, assessed and governed risk with a defined treatment plan	Risk register entries with named owners; documented prioritisation method; accepted-risk schedule with replacement dates
A3 — Asset management	Cryptographic assets understood as part of the asset base, tied to lifecycle and replacement planning	CBOM linked to the asset register; firmware verification capability recorded per asset class
A4 — Supply chain	Cryptographic dependencies in supplied products identified and contractually managed	Amended specifications; supplier readiness assessment; annual supplier roadmap returns
B2 — Identity and access control	Device and user identity dependent on signature schemes; remote access as the highest-consequence pathway	Remote access migration record; device identity scheme documentation; PKI migration plan
B3 — Data security	Protection of data in transit and at rest proportionate to its sensitivity lifetime	Long-lived data classification; encryption standard; third-party sharing controls for models and site documentation
B4 — System security	Integrity of software and firmware; secure configuration and update mechanisms	Signing estate map; firmware verification requirements; pilot results; exception register
B5 — Resilient networks and systems	Migration executed without degrading operational availability	Constrained-link test results; documented exemptions with justification; change and rollback records
B6 — Staff awareness and training	Engineering, procurement and architecture capability to apply the requirements	Training record for the named roles; specification review evidence
D1 — Response and recovery planning	Ability to respond to a cryptographic compromise or accelerated deprecation	Cryptographic incident scenario in the exercise programme; documented key and certificate replacement procedures

Board reporting

The Audit and Risk Committee does not need algorithm names. It needs to know whether the exposure is bounded, whether it is being closed at an adequate rate, and whether the money will be there when it is needed. Five measures carry that.

Measure	Definition	Why the board should care
Discovery coverage	Percentage of the estate with a completed cryptographic inventory, reported separately for IT, OT and supplier-delivered assets, with confidence level	A single blended figure conceals the OT gap; the split is the point
Tier-one asset status	Number of tier-one assets migrated, planned, or accepted as residual risk	Direct measure of whether the highest-consequence exposure is closing
Procurement compliance	Percentage of OT and telemetry contracts awarded in the period containing the cryptographic clauses	Measures whether the problem is still growing — the most actionable number on the list
Supplier readiness	Percentage of tier-one suppliers who have provided a dated post-quantum roadmap	Supplier timing is the principal external constraint on the plan
Funding position	Status of the post-quantum requirement within AMP9 planning and the PR29 submission	The one measure that determines whether the rest is deliverable

The narrative to accompany the numbers -

Our cryptography will need to change, on a national timetable, during the life of assets we are installing today. We do not know when the underlying threat becomes real and we are not managing to a threat date; we are managing to the asset and funding cycle, which we do control. The controllable actions are to stop installing the problem, which is a procurement change we are making now at negligible cost, and to complete discovery early enough to fund the migration properly at PR29. Where plant cannot be made quantum-resistant we will hold a documented, bounded set of accepted risks with compensating controls and replacement dates, and report it annually.

Conclusion

For UK water utilities, post-quantum cryptography is not primarily a future technology challenge. It is a governance, asset lifecycle, and investment planning challenge that must be addressed during AMP8 if organizations expect to meet both regulatory expectations and the NCSC migration timeline. The critical decision point is not 2035, but 2027-2028, when AMP9 funding submissions are developed and submitted through PR29.

The greatest risk does not lie in the confidentiality of operational data, but in the long-term integrity of operational technology assets, firmware trust chains, device identities, and remote access mechanisms that will remain in service well into the 2040s. Decisions made during today's procurement cycles will determine whether these assets can be transitioned to quantum-resistant security models or become future capital replacement liabilities.

The most successful water companies will not treat post-quantum cryptography as a standalone program. Instead, they will embed cryptographic requirements into existing AMP8 and AMP9 investment streams, establish a comprehensive cryptographic inventory across IT, OT and supplier ecosystems, and ensure that future operational technologies are procured with verifiable quantum-resilient migration paths.

Executive leadership should therefore focus on five outcomes over the next 24 months:

- Establish a funded and governed roadmap aligned to PR29 and AMP9 planning.
- Stop introducing future cryptographic debt through current procurement decisions.
- Build a defensible cryptographic inventory and Cryptographic Bill of Materials (CBOM).
- Prioritize authenticity, software trust and firmware signing over broad encryption refresh programmes.
- Align investments with NCSC and NIST standards while avoiding unproven or proprietary "quantum-proof" technologies.

Board Position

Post-quantum security should be viewed as an asset resilience program, not an encryption upgrade. Our objective is to prevent future operational risk by ensuring that the infrastructure we procure today remains secure, supportable, and defensible throughout its lifecycle. By completing discovery and funding planning during AMP8, we can meet regulatory expectations, protect long-lived operational assets, and deliver a controlled, risk-based transition to the post-quantum era without disrupting critical water services.

References

Primary standards and official guidance only. Vendor and commentary sources have been excluded deliberately; where a claim in this document rests on sector commentary rather than a primary source it is identified as such in the text.

1. NCSC, Timelines for migration to post-quantum cryptography, March 2025 — ncsc.gov.uk/guidance/pqc-migration-timelines
2. NIST, FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM), August 2024 — csrc.nist.gov/pubs/fips/203/final
3. NIST, FIPS 204, Module-Lattice-Based Digital Signature Standard (ML-DSA), August 2024 — csrc.nist.gov/pubs/fips/204/final
4. NIST, SP 800-208, Recommendation for Stateful Hash-Based Signature Schemes — csrc.nist.gov/pubs/sp/800/208/final
5. NCSC, Cyber Assessment Framework v4.0, August 2025 — ncsc.gov.uk/collection/cyber-assessment-framework
6. Drinking Water Inspectorate, The Network and Information Systems (NIS) Regulations 2018 — dwi.gov.uk/the-network-and-information-systems-nis-regulations-2018
7. UK Parliament, Cyber Security and Resilience (Network and Information Systems) Bill, introduced 12 November 2025; Commons stages completed and passed to the Lords, June 2026 — status should be confirmed at bills.parliament.uk
8. NIST, What Is Post-Quantum Cryptography? — nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography
9. NSA, Quantum Key Distribution (QKD) and Quantum Cryptography (QC) — nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC
10. NIST, Considerations for Achieving Crypto Agility (CSWP 39) — csrc.nist.gov/pubs/cswp/39
11. OWASP CycloneDX — cryptographic bill of materials; published as ECMA-424 — cyclonedx.org/capabilities/cbom
12. NIST NCCoE, Migration to Post-Quantum Cryptography project — nccoe.nist.gov — migration to PQC
13. CISA, Post-Quantum Considerations for Operational Technology — cisa.gov/resources-tools/resources/post-quantum-considerations-operational-technology
14. NIST, IR 8547 (initial public draft), Transition to Post-Quantum Cryptography Standards — csrc.nist.gov/pubs/ir/8547/ipd
15. NIST, Cybersecurity Framework 2.0 — nist.gov/cyberframework

About this document. Prepared by Infosys Cybersecurity, C&A Cyber IoT/OT. This Point of View is advisory and reflects published standards and guidance current at July 2026. Regulatory status — in particular the passage of the Cyber Security and Resilience Bill and the profile designated by the competent authority — should be verified before the document is relied upon. Asset lives, retention periods and capital planning dates are stated as planning assumptions and should be confirmed against the undertaker's own asset management plan, records retention schedule and regulatory calendar.

About the Author

Michel Bruggeman

Principal Consultant | EMEA IoT & OT Lead

Michel Bruggeman is a distinguished cybersecurity leader with over 25 years of experience, specializing in Operational Technology (OT) security, industrial cybersecurity architecture, and cyber resilience. He has held strategic roles across the insurance, manufacturing, energy, and semiconductor sectors, focusing on ICS/OT risk assessments, secure cloud adoption, and incident response readiness. Michel is a SANS /ISA Mentor and Microsoft Certified Trainer, with deep expertise in IEC 62443, DORA, NIS2, NIST, and ISO 27001.

For more information, contact askus@infosys.com

Infosys®
Navigate your next