



Dŵr Cymru
Welsh Water

Enhanced Investment
Case:
WSH57-CS01 –
Increasing Physical and
Cyber Security



Contents

- Executive Summary 3
- 1. Introduction 5
 - 1.1 Physical Security 5
 - 1.2 Cyber Security 5
 - 1.3 Structure of this Document 7
- 2. Physical Security 9
 - 2.1 Need for Enhancement Investment 9
 - 2.2 Best Option for Customer 12
 - 2.3 Costing Efficiency 16
 - 2.4 Providing Customer Protection 17
- 3. Cyber Security 18
 - 3.1 Need for Enhancement Investment 18
 - 3.2 Best Option for Customer 20
 - 3.3 Costing Efficiency 26
 - 3.4 Providing Customer Protection 26
- 4. Appendix A 28

Executive Summary

This investment will improve the security of the Welsh Water estate – both in terms of physical security of assets and cyber security of networks, systems and data.

In both areas, we are required to meet various laws and government-mandated standards. The proposed enhancement spend will ensure we are compliant with the regulatory standards, are agile in responding to the challenging and evolving threat landscape and that security risks are reduced to the lowest practicable level.

We have structured this document using the enhancement assessment criteria set out in Ofwat's PR24 Final Methodology, Appendix 9 (Setting Expenditure Allowances), Section A1. The enhancement assessment criteria are divided into four criteria groupings:

- Need for enhancement investment
- Best option for customers
- Cost efficiency, and
- Customer protection

Need:

Physical Security: The proposed programme of work ensures that the security of all assets meets the UK government's statutory Security and Emergency Measures Direction (SEMD) regulatory standards (under section 208 of the Water Industry Act 1991).

In addition, all Critical National Infrastructure (CNI) assets are required to meet a series of government regulations and standards. These regulations include:

- National Protective Security Authority (NPSA),
- Water UK Security Standards (WUKSS)
- Occupiers Liability Act (1984).

As part of a programme of work conducted by the Cabinet Office into criticalities, Welsh Ministers and Welsh Water undertook a review of CNI classifications to establish whether our current CNI lists reflect the true essential functions across our asset base. This resulted in an additional 18 Welsh Water sites being newly identified with CNI status. Whilst there is a level of security at these sites appropriate to their previous status, a programme of work is required to enhance these sites to CNI standards. Un-addressed, this would expose Welsh Water to both material and legal risks.

The proposed investment, agreed with the Welsh Government and DWI, is based on bringing all non-complaint security assets up to the mandated SEMD standards.

Cyber Security: It is a legal requirement for all companies providing Essential Services in the UK (including water companies) to conform to the Network & Information Systems Regulations (NIS - R), 2018.

It is recognised that cyber threats are continuously evolving making it difficult to predict the nature of future potential attacks. This necessitates constant vigilance and the ability to react rapidly to emerging threats.

The proposed investment is based on ensuring that all relevant systems and data have sufficient security controls to meet the required regulatory standards, and that suitable measures are in place to protect from currently known threats, while also maintaining the ability to react to newly identified threats.

Options:

For both physical and cyber security, several options were considered. All options are constrained by the mandated minimum standards and regulations imposed by regulatory bodies.

We have worked closely with government departments to confirm the proposed solutions.

What We Will Deliver:

For the physical security enhancements, this will require upgrades to: Fences, Intruder Alarms, Doors, Window Bar sets and CCTV across 11 sites.

For cyber security, the work will include Extended Detect and Respond (XDR) solutions and Enhanced Security Operations Centre (SOC) Security Information and Event Management (SIEM) capability across Operational Technology (OT) environments.

Efficient Costing:

Where possible, costing has been performed using a “bottom-up” approach. Costs were based upon historic trend analysis and extrapolation of historic data. The costing methodology has been reviewed and assured by an independent third party.

We will deliver £34M (post efficiency, 2022/23 price base) of investment across these two measures.

Customer Protection:

This work will be delivered with strong oversight from Welsh Government within a well-established legislative and regulatory structure. The chosen options - under NIS and SEMD - have been agreed with the Welsh Government and DWI and will be enforced.

1. Introduction

In this document, we make the case for investing in enhanced security measures to protect against increasing security threats.

Our plans cover both physical security (see Section 2) and cyber security (see Section 3).

1.1 Physical Security

The proposed programme of work ensures that the security of all assets meets the UK government's statutory Security and Emergency Measures Direction (SEMD) regulatory standards (under section 208 of the Water Industry Act 1991).

This enhancement will modernise and improve the physical security of Welsh Water sites and assets, providing both protection for the assets and, importantly, maintaining a reliable supply of safe drinking water for the public.

The key areas and costs are shown in Table 1.

Table 1: Enhancement Costs for Physical Security

Item	TotEx*
CNI Upgrades	£12.533M
Water UK Security Standards	£10.936M
Total	£23.469M

** post frontier shift and real price effects, and in 2022/23 price base*

The programme will ensure that Welsh Water assets are secured from intruders, thus reducing the risk of death or serious injury to members of the public – in line with Welsh Water's responsibilities under the Occupiers Liability Act (1984). It also protects sites from vandalism, thus maintaining a safe working environment as required by the Health and Safety at Work Act (1974), and it reduces the risk of malicious contamination or disruption of the water supply (SEMD).

1.2 Cyber Security

This enhancement case will improve Welsh Water's Cyber Security capabilities and reduce the cyber risk across the organisation. The enhancement will also ensure that all Welsh Water's systems and networks meet our target maturity level against the Centre for Internet Security (CIS) recommended Critical Security Controls for cyber security – commonly known as CIS 18.

Specific activities include:

- Extended Detect and Respond (XDR) solutions for Operational Technology (OT) environments.
- Enhanced Security Operations Centre (SOC) Security Information and Event Management (SIEM) capability extended across OT environments.

- Cyber culture maturity improvements to reduce people-related cyber risks, including targeting high risk and privileged access users as well as evolution of phishing and other technology security practice campaigns to reflect latest attacker techniques.
- Next Generation Cyber Threat Intelligence capabilities, leveraging developments in AI & Machine Learning, enabling us to develop our defensive strategies against ongoing changes in the cyber threat landscape.
- Enhancements in Identity and Access Management (IDAM) capability, include but are not limited to:
 - Auto-enrolment and auto-decommissioning of identity and access for employees, contractors, and partners.
 - Evolution of single-sign-on (SSO) to address threat landscape.
 - Robust, comprehensive, complete and consistent Multi Factor Authentication (MFA) across IT and OT environments.
 - Appropriate and consistently deployed controls for privileged access management.
- Enhanced third party security management capabilities to provide visibility and mitigation of cyber risks associated with supply chain compromises.

The key areas and costs are shown in Table 2.

Table 2: Enhancement Costs for Cyber Security

Item	TotEx*
Cyber Security	£11.054M

** post frontier shift and real price effects, and in 2022/23 price base*

1.3 Structure of this Document

We have structured this investment case using the enhancement assessment criteria set out in Ofwat's PR24 Final Methodology, Appendix 9 (Setting Expenditure Allowances), Section A1.1:

ID from Appendix 9	Abbreviated Assessment Criterion	Addressed In	
		Physical Security	Cyber Security
A1.1.1 Need for enhancement investment	a Is there evidence that the proposed investment is required?	Section 2.1.1	Section 3.1.1
	b Is the scale and timing of the investment fully justified?	Section 2.1.1	Section 3.1.1
	c Does the proposed investment overlap with base activities?	Section 2.1.2	Section 3.1.2
	d Does the need and/or proposed investment overlap/duplicate with previously funded activities or service levels?	Section 2.1.3	Section 3.1.3
	e Does the need clearly align to a robust long-term delivery strategy within a defined core adaptive pathway?	Section 2.1.4	Section 3.1.4
	f Do customers support the need for investment?	Section 2.1.1	Section 3.1.1
	g Have steps been taken to control costs, including potential cost savings?	Section 2.1.5	Section 3.1.5
A1.1.2 Best option for customers	a Have a variety of options with a range of intervention types been explored?	Section 2.2.1	Section 3.2.1
	b Has a robust cost-benefit appraisal been undertaken to select the proposed option?	Section 2.2.1	Section 3.2.1
	c Has the carbon impact, natural capital and other benefits that the options can deliver been assessed?	Section 2.2.2	Section 3.2.2
	d Has the impact of the proposed option on the identified need been quantified?	Section 2.2.2	Section 3.2.2
	e Have the uncertainties relating to costs and benefit delivery been explored and mitigated?	Section 2.2.3	Section 3.2.3
	f Where required, has any forecast third party funding been shown to be reliable and appropriate?	Not applicable for this case	Not applicable for this case
	g Has Direct Procurement for Customers (DPC) delivery been considered?	WSH50-IP00 Our Approach to Investment Planning	WSH50-IP00 Our Approach to Investment Planning
	h Have customer views informed the selection of the proposed solution?	Section 2.2.4	Section 3.2.4

ID from Appendix 9	Abbreviated Assessment Criterion	Addressed In	
		Physical Security	Cyber Security
A1.1.3 Cost efficiency	a Is it clear how the company has arrived at its option costs?	Section 2.3.1	Section 3.3.1
	b Is there evidence that the cost estimates are efficient?	Section 2.3.2	Section 3.3.2
	c Does the company provide third party assurance for the robustness of the cost estimates?	Section 2.3.1	Section 3.3.1
A1.1.4 Customer protection	a Are customers protected if the investment is cancelled, delayed or reduced in scope?	Section 2.4	Section 3.4
	b Does the protection cover all the benefits proposed to be delivered and funded?	Section 2.4	Section 3.4
	c Does the company provide an explanation for how third-party funding or delivery arrangements will work for relevant investments?	Not applicable for this case	Not applicable for this case

2. Physical Security

2.1 Need for Enhancement Investment

This section sets out the drivers behind the need and urgency for change and describes the context within which it has arisen. We describe the strong regulatory framework which drives action as threats continue to emerge and evolve.

2.1.1 Evidence that Enhancement is Needed

Is there evidence that the proposed enhancement investment is required?

Is the scale and timing of the investment justified?

Where appropriate, is there evidence that customers support the need for investment?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.1a, A1.1.1b and A1.1.1f

On 1 March 2022, The Security and Emergency Measures (Water and Sewerage Undertakers and Water Supply Licensees) Direction 2022 (SEMD 2022) came into effect. In terms of governance, both DEFRA and Welsh Ministers have agreed to delegate operational powers for SEMD to the Drinking Water Inspectorate (DWI). This approach, like that for the NIS Regulations, sees Welsh Ministers still retain the overall governance of the legislation whilst DWI undertake the assessment of RAG submissions, conduct audits, and issue enforcement.

All water CNI sites must conform to the SEMD regulatory standards. In addition, they must comply with the standards agreed with UK Government specifically:

- NPSA and their guidance for CNI assets.
- Protective Security Guidance (PSG) issued by Welsh Government (January 2023).
- The WUKSS (January 2023), as a baseline set of controls.
- Occupiers Liability Act (1984).

As part of a wider review into criticalities being undertaken by the Cabinet Office, Welsh Government formally requested Welsh Water to perform a review to assess CNI assets within our estate. This request was made in a meeting between Welsh Water and the Head of Water Branch, Welsh Government and the Water Security & Resilience Programme Manager, (Water and Flood Division), Welsh Government, in October 2022.

We presented a series of proposals based on the work completed in England and our own internal requirements.

In August 2023, Welsh Ministers agreed with our proposed criteria for the designation of assets to CNI status:

1. An asset normally supplies a population of >350,000 and performs one of the SEMD functions listed in PSG i.e., supply raw water (including transfer and storage), water treatment and distribution of treated water.
2. In exceptional circumstances, the population threshold of >100,000 may be applied to the designation to CNI status of those assets that are of strategic importance to the region they serve,

do not have alternative water treatment services capable of deployment to fulfil water demand in the event of asset failure and are a single point of failure.

3. Alarm monitoring centres (AMC) are no longer required to be designated as CNI assets.
4. The Wastewater treatment works that have been a designated CNI site for several years will continue to retain their CNI status due to their strategic significance to the river they discharge to. This is acknowledged and accepted as a departure from the CNI designation criteria in PSG.

As a result of these proposals an extra 18 assets within Welsh Water will now be designated CNI status and hence require security measures to be upgraded to CNI standard.

Within the SEMD self-assessment process there are specific security outcomes covering CNI and associated risks. Whilst we currently are at “Green” status, the inclusion of these additional sites will require the outlined investment to maintain that status across the AMP.

The required upgrades include improved fences, intruder alarms, doors, window bar sets and CCTV. The issue list was submitted to the Welsh Government and the DWI on the 20th of March 2023.

The DWI has formally endorsed the need for all the CNI upgrades and has provided letters of support for each of the proposed upgrades. (Letters of support are from the DWI Deputy Chief Inspector, on behalf of the Welsh Ministers). These schemes of work will be individually covered by a section 19 Undertaking issued by DWI to Welsh Water.

The proposed investment is based on bringing all non-complaint security assets up to the mandated SEMD standards.

Our approach to customer engagement is set out in Stepping up to the Challenge: Business Plan 2025-30 (Section 2.2). We have not engaged with customers on these issues as they are legislatively driven and security sensitive.

2.1.2 [Overlap with Activities to be Delivered through Base](#)

Does the proposed enhancement investment overlap with activities to be delivered through base?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.1c

Our approach to separating base and enhancement is set out in WSH50-IP00 Our Approach to Investment Planning.

The investment values are distinctly identified as either base or enhancement:

- At sites with no existing CNI infrastructure, all the costs have been allocated to enhancement.
- All newly identified CNI sites are compliant with Water UK Security Standards (WUKSS). As a result of these sites being upgraded to CNI categorisation, additional and enhanced security measures will be required to be installed to comply with CNI guidance. The costs of these upgrades have been allocated to enhancement. The costs of maintaining existing assets (such as hatch alarms) are allocated to the base allowance and are therefore out of scope of this enhanced investment case.

In total, 18 sites have been identified as needing enhancement as CNI sites. For 7 of these sites, work has already been performed using existing capital, thus limiting the further required enhancement investment to 11 sites.

There are various risk control measures covered by base at all sites (regardless of CNI categorisation). Many of these are to promote behavioural management to protect against threats. These include:

- Ensuring all sites have access controls, both at site entry and for controlled areas.
- Maintaining a clean desk policy.
- Ensuring security measures are not circumvented for convenience (e.g., security doors are not left propped open).
- Putting measures in place to prohibit tailgating at security gates.
- Undertaking risk-based audits to identify learning and maintain the security culture across sites.
- Conducted security related exercises, mandatory at CNI sites but risk based across all other sites.
- Full personal security campaign which also includes good cyber security hygiene.

We strive to maintain excellent security practices, which are a foundation onto which the enhanced investment builds.

2.1.3 [Overlap with Funding from Previous Price Reviews](#)

Does the need and/or proposed enhancement investment overlap with activities or service levels already funded at previous price reviews?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.1d

In AMP7 we were funded to deliver activity at 90 sites to maintain compliance with SEMD, this work is on track to be delivered and is distinct from the activities identified for AMP8.

In relation to this, Welsh Water is required to submit to the DWI and Welsh Ministers an annual RAG assessment stating, the level of compliance with SEMD across a range of security outcomes. The most recent submission was made in March 2023. This mechanism ensures that previous funding has been invested to deliver required outputs and clearly articulates new requirements.

2.1.4 [Alignment with the Long Term Delivery Strategy](#)

Is the need clearly identified in the context of a robust long-term delivery strategy within a defined core adaptive pathway?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.1e

Welsh Water’s document WSH01 Long Term Delivery Strategy specifically identifies physical security requirements. Due to overarching nature of this investment type, it is not aligned to specific outputs of the company and therefore does not form part of Welsh Water’s 2050 output measures.

Due to the importance that physical security plays in facilitating the 2050 long term outputs it has been called out separately in Welsh Water’s document WSH01 Long Term Delivery Strategy. A core pathway has been developed which reflects the physical security elements which are explained in more detail in

the Long Term Delivery Strategy. The core pathway assumes no changes to current legislation and as such no additional SEMD enhancement security is forecast beyond AMP8 as by this time investment plans should ensure all sites across the Welsh Water network are in line with current SEMD expectations. Any replacement of existing SEMD assets will form part of a base maintenance plan which is outside of the current Long Term Delivery Strategy.

Alternative pathways have been created, although due to materiality are not included as part of data tables LS3/4 A-J.

2.1.5 Management Control of Costs

Is the investment driven by factors outside of management control? Is it clear that steps been taken to control costs and have potential cost savings been accounted for?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.1g

The new SEMD regulations were published in 2022 (see Water Industry Act 1991: Section 208, The Security and Emergency Measures Direction 2022), so changes to security standards are new to the industry and require a prompt response.

In the SEMD 2022 document, clauses 7 to 13 have been added – they are new requirements that did not previously exist. These include new requirements relating to the identification and mitigation of security risks, approval and training of staff and testing of security measures.

Historic evidence has demonstrated that security upgrades for our assets have seen a reduction in the incidence of trespass and criminality and in ensuring the success of our day-to-day operations. This investment will therefore see an expansion of this positive outcome across further sites in AMP9.

2.2 Best Option for Customer

In this section, we describe how we have developed options for addressing the need identified above.

The optioneering process is delivered within strict regulatory guidance and in close collaboration with regulatory bodies. As such our standard principles, the TotEx hierarchy approach and cost benefit assessment, have only a marginal influence on the development of options.

Due to the security sensitive nature of this work, we will not present details of specific options.



2.2.1 Identification of Solution Options


Has the company considered an appropriate number of options over a range of intervention types to meet the identified need?

Is there evidence that the proposed solution represents best value for customers, communities, and the environment over the long term?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.2a and A1.1.2b

Table 3: Solution Options for Physical Security

Type of Option	Brief Description of Option and Comments	Potentially Viable, i.e., progress to shortlisting?
Eliminating, reducing or delaying the need for change	<p>Not viable.</p> <p>As described in Section 2.1.1, choosing not to change in the face of increasing security threats or choosing to only partially protect against known threats puts us in breach of a number of regulatory requirements. This is unacceptable - as set out in our Asset Management Policy, we are committed to complying with current and relevant statutory and regulatory requirements.</p>	
Maintaining the effective risk controls already in place	<p>Viable – <u>base</u> investment</p> <p>Keep existing arrangements in place, so that risks already under control remain in control. Examples of existing controls include, but are not limited, to:</p> <ul style="list-style-type: none"> - Continual programmes to raise awareness and train colleagues on security. - Protection against unauthorised access and deliberate or unintentional misuse of assets, systems, and information. <p>Ensuring that our physical security controls are maintained in good working order.</p> <p>This is foundational to the enhanced investment described in this case and is delivered through base allowance. On its own, it does not fully address the need described in Section 2.1.1.</p>	 <p>The costs and benefits of our base activities are included in our PR24 Plan and are outside the scope of this enhancement case.</p>

Type of Option	Brief Description of Option and Comments	Potentially Viable, i.e., progress to shortlisting?
Enhancing existing or adding new resources	<p>Step-change enhancement, such as introduction of new equipment or technology at a site, to transform the security capability.</p> <p>This includes the step-changes required at the newly designated CNI sites that do not currently comply with the minimum stipulated requirements. This includes enhancing the existing security hardware:</p> <ul style="list-style-type: none"> • Fences. • Intruder alarms. • Doors. • Window bar sets. • CCTV. <p>Additionally, new processes will need to be implemented for the CNI sites (such as reporting, processes, and auditing).</p>	

The approach to security options development is defined by legislation and conducted through close working with government teams.

Where appropriate, for each area of investment, the cost and risk of non-intervention has been assessed and at least two intervention options have been considered.

For the CNI sites the design is, in effect, mandated by the guidance provided by the NPSA (including legacy guidance, still in effect, from CPNI) and the Protective Security Guidance (PSG) issued by Welsh Ministers. Additional baseline controls are also outlined within the WUKSS (Version 4.2, January 2023).

2.2.1.1 Assessment and Selection of Solution Options

We have used our standard CBA approach, set out in WSH50-IP00 Our Approach to Investment Planning (Section 4.3), to evaluate the planned work. The results for the planned investment in WUKSS are shown in Table 4.

Table 4 shows that using our standard assessment the mandated work will not pay back within 30 years but will produce some benefits. This investment would be unlikely to be funded through base maintenance, but we have a statutory obligation to deliver this under an enhancement driver. This analysis reflects limitations in our CBA approach linked to low probability high consequences events - rather than capturing the true position of the proposed activity.

Table 4: Cost Benefit Analysis for AMP8 Enhanced Investment in WUKSS

Option Name	Initial CapEx*	Present Value Whole Life Costs* (WLC)	Present Value Whole Life Benefits* (WLB)	Benefit/Cost Ratio	Net Present Value* (=WLB-WLC)
Install security measures to ensure compliance with regulations and guidelines	£10.791M	£9.686M	£5.400M	0.558	-£4.285M

* pre frontier shift and real price effects, and in 2022/23 price base

Should a site be targeted by a terrorist organisation and security measures do not prevent access – destruction of assets on the site or deliberate contamination of water supplies could have significant repercussions for public health. It is difficult to quantify the likelihood of such an event and the consequences for society. Similarly, a non-malicious intrusion onto the site could lead to the serious injury or fatality of trespassers, this too is hard to quantify.

Fundamentally the work set out in this case and the options selected are mandated by Government action, whilst a CBA provides some insight into potential benefits it does not provide a basis on which to judge the strength of the case.

2.2.2 Quantification of Benefits

Has the company fully considered the carbon impact, natural capital and other benefits that the options can deliver?

Has the impact of the proposed option on the identified need been quantified, including the impact on performance commitments where applicable?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.2c and A1.1.2d

Our approach to benefit assessment is set out in WSH50-IP00 Our Approach to Investment Planning (Section 4.3). Section 3.2.2 below covers A.1.1.2c.

2.2.2.1 Quantifying the Impact on Need and Performance Commitments

By their nature, security measures have no direct measurable impact on the performance commitments.

The security measures will reduce the risk of catastrophic failure due to loss of a physical asset, either by criminal damage, sabotage, or terror-related incident.

These are low-likelihood, high-consequence events, and do not link through to annual performance targets.

2.2.3 Uncertainties relating to Cost and Benefit Delivery

Have the uncertainties relating to costs and benefit delivery been explored and mitigated? Have flexible, lower risk and modular solutions been assessed – including where forecast option utilisation will be low?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.2e

The SEMD and NPSA guidelines recommend specific minimum design standards, these are well understood in terms of their costs and benefits. The option that must be selected to deliver the required level of security (benefit) is defined by national guidance and agreed with DWI.

Since this investment case is made up of many low-cost solutions, at the individual project level there is cost and benefit risk. However, at the aggregate level there is a high level of confidence that the benefits are achievable, and the costs are controllable.

2.2.4 Involving Customers in Option Selection

Where appropriate, have customer views informed the selection of the proposed solution, and have customers been provided sufficient information (including alternatives and its contribution to addressing the need) to have informed views?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.2h

It is not appropriate to consult with customers on the details of security design options. We have worked closely with the government departments – DWI/DEFRA – to confirm the proposed solutions.

2.3 Costing Efficiency

In this section we give details on our approach to costing. Our overarching approach to developing efficient costs is set out in WSH50-IP00 Our Approach to Investment Planning (Section 4.10).

2.3.1 Developing a Cost for Security

Is it clear how the company has arrived at its option costs? Is there supporting evidence on the calculations and key assumptions used and why these are appropriate?

Does the company provide third party assurance for the robustness of the cost estimates?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.3a and A1.1.3c

We costed CCTV and perimeter intrusion detection systems bottom-up, as described in WSH50-IP00 Our Approach to Investment Planning, using quotations from our current suppliers. Working with our suppliers we can understand the potential scope of works which can be quantified and costed using work item rates. This approach is appropriate as it provides us with a more robust cost, where we do not hold sufficient historical project cost data ourselves.

Other CNI upgrades were again costed using a bottom-up approach using rates generated from historical projects. We have a sufficient understanding of costs for this work, and we can therefore use this to understand future expenditure. We can develop and quantify a scope of works for the AMP and therefore use rates adjusted for date using CPIH, to generate a programme cost.

Protecting National Infrastructure assets to WUKSS were costed using historic trend analysis and extrapolation based on our previous expenditure as described in our Costing Methodology. Specific interventions and volume have not fully been established but we have well-established patterns of spending in the past, which is an appropriate approach to inform future expenditure for lower cost items.

Along with our overall costing strategy being reviewed and assured by Jacobs, we have also employed third party consultants to review enhancement cases to provide confidence that the estimates within them are robust, efficient and deliverable.

2.3.2 Benchmarking Our Approach

Is there evidence that the cost estimates are efficient (for example using similar scheme outturn data, industry and/or external cost benchmarking)?

– *Ofwat's final methodology for PR24, Appendix 9, A1.1.3b*

Designs are standardised across the industry and costs are generally restricted given the secure nature of the work being undertaken.

2.4 Providing Customer Protection

Are customers protected if the investment is cancelled, delayed or reduced in scope?

Does the protection cover all the benefits proposed to be delivered and funded?

– *Ofwat's final methodology for PR24, Appendix 9, A1.1.4a and A1.1.4b*

This area has strong oversight from UK and Welsh Government.

It is a requirement of the regulations that an annual audit be made of the emergency planning and security capabilities of Welsh Water. This is submitted to Welsh Ministers and DWI at the end of March each year. As part of the security aspect, there are specific assessment areas for NI and CNI assets, including a requirement that a statement be made confirming that all CNI assets comply with the SEMD requirements or are in an approved process of upgrading their protection to comply. This is a requirement of SEMD (2022), sections 17 and 18. This reporting process tracks progress across our SEMD compliance.

As part of this SEMD self-assessment, all CNI sites also require an annual audit to be completed to demonstrate security compliance, which is then submitted to Welsh Ministers and DWI. These audits need to be completed in accordance with guidance within the PSG can be undertaken by appropriately trained staff within Welsh Water or by an external consultant (who is a NPSA/RSES registered auditor). The most recent audit was completed in October 2022 by an external consultant.

3. Cyber Security

3.1 Need for Enhancement Investment

This section sets out the drivers behind the enhancement case and describe the context within which it has arisen. We describe the strong regulatory framework which drives action as threats continue to emerge and evolve.

3.1.1 Evidence that Enhancement is Needed

Is there evidence that the proposed enhancement investment is required?

Where appropriate, is there evidence that customers support the need for investment?

Is the scale and timing of the investment justified?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.1a, A1.1.1b and A1.1.1f

It is a legal requirement for all companies providing essential services in the UK (including water companies) to conform to the Network & Information Systems regulations (2018).

Welsh Water has developed an action plan to meet the Target Sector Profile for the Cyber Assessment Framework (CAF) for UK water companies by the end of the current AMP, i.e., March 2025.

Additionally, the DWI has recently published and an enhanced Cyber Assessment Framework (eCAF), requiring additional improvements to six of the contributing outcomes by March 2028. Further details can be found in the letter from DWI (Deputy Chief Inspector of Drinking Water), 23 June 2023. The eCAF is already directly applicable for activity in England with a Welsh equivalent being confirmed with Welsh Government.

There will be an ongoing requirement to further develop our Cyber capabilities to maintain the required level of compliance set out in NISR.

In addition, it is anticipated that the scope of NISR will be extended to cover Wastewater operations during AMP 8. This will require appropriate systems and processes to be extended across these business areas to comply with the wider operational scope.

Welsh Water has adopted the Centre for Internet Security (CIS) 18 Critical Security Controls framework as the minimum standard to which all IT and OT systems and activities will be held. This is an internationally recognised set of controls and is the adopted standard by several international organisations, including the European Telecommunications Standards Institute (ETSI).

Welsh Water has a stated strategic objective of improving the overall Cyber Maturity score against the CIS 18 Maturity Matrix (a 5-point scale). To enable this, Welsh Water has compiled a set of Key Risk Indicators which have been used to highlight the areas which require enhanced investment and to define the Cyber Programme.

Our approach to customer engagement is set out in Stepping up to the Challenge: Business Plan 2025-30 (Section 2.2). We have not engaged with customers on these issues as they are driven by risk and regulation and the details are sensitive from a confidentiality perspective.

Given the current threat landscape, defined as Critical by NCSC in April 2023, and with no anticipated easing of threat levels, the scale and the timing of the investment are not only justified but recommended by NCSC and HMG.

3.1.2 Overlap with Activities to be Delivered through Base

Does the proposed enhancement investment overlap with activities to be delivered through base?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.1c

Our approach to separating base and enhancement is set out in WSH50-IP00 Our Approach to Investment Planning (Section 3.4).

We have an ongoing base investment program to maintain the digital security of our assets against existing threats. Base investment is key in maintaining the security of our estate to known threats. The investment set out here is specifically to meet new requirements and move us to a posture which is appropriate for the evolving threat landscape.

3.1.3 Overlap with Funding from Previous Price Reviews

Does the need and/or proposed enhancement investment overlap with activities or service levels already funded at previous price reviews?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.1d

In AMP7, the programme has delivered several foundational capabilities in the OT domain, including a revised network architecture and deployment of a dedicated ‘demilitarised zone’ (DMZ) within the OT environment. There have also been a significant number of process and procedural improvements, such as the deployment of OT cyber incident response capability, to assist with forensic analysis of cyber incidents across the distributed asset base at operational sites.

The IT Cyber Programme implemented high priority remediation activities that needed to be addressed across the technology estate. Cyber-attacks against OT typically originate in IT environments, hence the focus during AMP7 on ensuring our perimeter and corporate controls are robust - we have put in place a strong foundation on which to build the enhanced developments both in IT and OT environments.

3.1.4 Alignment with the Long-Term Delivery Strategy

Is the need clearly identified in the context of a robust long-term delivery strategy within a defined core adaptive pathway?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.1e

Welsh Water’s document WSH01 Long Term Delivery Strategy specifically identifies cyber security requirements. Due to the broad and responsive nature of this investment type, it is not aligned to specific outputs of the company and therefore does not form part of Welsh Water's 2050 output measures.

Due to the importance that cyber security plays in facilitating the 2050 long term outputs it has been called out separately in Welsh Water's document WSH01 Long Term Delivery Strategy. A core pathway has been developed which reflects the cyber security elements which are explained in more detail in the Long Term Delivery Strategy report.

There is no cyber security investment within the core pathway beyond AMP8 due to the uncertain and evolving nature of the requirements in this area. For example, it is not yet clear what impact will be felt by developments such as Generative AI/ Large Language Models and quantum computing.

Alternative pathways have been created for both investment areas, although due to materiality are not included as part of data tables LS3/4 A-J.

3.1.5 Management Control of Costs

Is the investment driven by factors outside of management control? Is it clear that steps been taken to control costs and have potential cost savings been accounted for?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.1g

Cyber security is a continuously evolving discipline. The number of cyber threats continues to increase, and the nature of the threats is constantly changing, including risks from foreign state actors and organised crime groups. The changes of these threats are outside of management control and necessitate constant vigilance and proactive preventative, detective and responsive measures.

Additionally, there are often updates to legislation mandating measures that require investment. These, too, are outside of management control.

Within the existing estate, we have a suite of security controls in place to prevent, detect and respond to known threats. These controls have been selected for their appropriateness to the threat type and range from automated handling of threat events through to more resource-intensive interventions. Our approach is to utilise the most appropriate and effective measure for each threat type, rather than an indiscriminate “one-size-fits-all” approach. These existing measures are funded through base.

The enhanced investment, as in this case, is intended to address more sophisticated attempts by threat actors to compromise IT and OT environments. It is intended to raise the overall security posture of our technology and to be agile in responding to the evolving threat landscape.

3.2 Best Option for Customer

In this section, we describe how we have developed options for addressing the need identified above.

The optioneering process is delivered within strict regulatory guidance and in close collaboration with regulatory bodies. As such our standard principles, the TotEx hierarchy approach and cost benefit assessment, have only a marginal influence on the development of options.

Due to the security sensitive nature of this work, we will not present details of specific options.

3.2.1 Identification of Solution Options

Has the company considered an appropriate number of options over a range of intervention types to meet the identified need?

Is there evidence that the proposed solution represents best value for customers, communities, and the environment over the long term?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.2a and A1.1.2b


The approach to security options development is defined by legislation and conducted through close working with government teams.


Various options have been considered within the constraints of the NIS. These options included investment strategies of:


- Regress (no further spend on a particular area).
- Maintain and Optimise (focussing on maintaining existing systems and technologies).
- Transform – Technology (focussing on cyber maturity improvements).
- Transform – Process (focussing on improvements to security processes).

For each investment strategy, specific implementation activities were identified, and a benefits/drawbacks assessment was performed. This assessment then informed the decision-making process for the proposed spend.

Table 5: Solution Options for Cyber Security

Type of Option	Brief Description of Option and Comments	Potentially Viable, i.e., progress to shortlisting?
Eliminating, reducing or delaying the need for change	Not viable. The emergence of new security threats is not under our direct control or influence. As described in Section 3.1.1, choosing not to change in the face of increasing security threats or choosing to only partially protect against known threats puts us in breach of the Network & Information Systems regulations (2018). This is unacceptable - as set out in our Asset Management Policy, we are committed to complying with current and relevant statutory and regulatory requirements.	

Type of Option	Brief Description of Option and Comments	Potentially Viable, i.e., progress to shortlisting?
<p>Maintaining the effective risk controls already in place</p>	<p>Keep existing arrangements in place, so that risks already under control remain in control.</p> <p>Examples of existing controls include but are not limited to:</p> <ul style="list-style-type: none"> - Continual programmes to raise awareness and train colleagues on cyber security. - Protection against unauthorised access and deliberate or unintentional misuse of IT systems and electronic information on-site or remotely, by colleagues and external stakeholders (e.g., user account management; governance and control on file sharing). - Ensuring that our IT systems and data platforms are maintained and kept up-to-date with security patches for known threats. This includes our AMP8 plans to provide SCADA, PLC and outstation replacements. Following its detailed assessment of our plans, the DWI has confirmed their support (refer to the DWI letter about DWI reference NIS DWR_01 dated 31 August 2023, sent to Welsh Water and copied to Paul Martin at Ofwat). - Eliminating redundant IT systems. <p>This is foundational to the enhanced investment described in this case and is delivered through base allowance. On its own, it does not fully address the need for change as expected under the Network & Information Systems regulations (2018).</p>	<div style="text-align: center;">  </div> <p>The costs and benefits of our base activities are included in our PR24 Plan and are outside the scope of this enhancement case.</p>

Type of Option	Brief Description of Option and Comments	Potentially Viable, i.e., progress to shortlisting?
<p>Enhancing existing or adding new resources</p>	<p>Step-change enhancement, such as introduction of a new technology, in order to transform the security capability and to better handle new and emerging threats.</p> <p>Examples of new controls include:</p> <ul style="list-style-type: none"> - Extended Detect and Respond (XDR) solutions for Operational Technology (OT) environments. - Enhanced Security Operations Centre (SOC) Security Information and Event Management (SIEM) capability extended across OT environments. - Cyber culture maturity improvements to reduce people-related cyber risks, including targeting high risk and privileged access users as well as evolution of phishing and other technology security practice campaigns to reflect latest attacker techniques. - Next Generation Cyber Threat Intelligence capabilities, leveraging developments in AI & Machine Learning, enabling us to develop our defensive strategies against ongoing changes in the cyber threat landscape. - Enhancements in Identity and Access Management (IDAM) capability, including but not limited to: <ul style="list-style-type: none"> o Auto-enrolment and auto-decommissioning of identity and access for employees, contractors and partners. o Evolution of single-sign-on (SSO) to address threat landscape. o Robust, comprehensive, compete and consistent Multi Factor Authentication (MFA) across IT and OT environments. - Enhanced third party security management capabilities to provide visibility and mitigation of cyber risks associated with supply chain compromises. <p>These measures would require enhanced investment to implement, and they build upon the foundational elements that we have put in place.</p>	

We have scaled the investment to match previous levels of activity and considered typical options that will be deployed. The changing nature of the threat will require options to evolve in period to respond to new hazards.

3.2.1.1 Assessment and Selection of Solution Options

Several intervention and non-intervention options have been considered which highlight the risks and costs of taking no action versus the costs of taking appropriate action.

Table 6 shows the results of our CBA analysis for cyber security.

Table 6: Cost Benefit Analysis for AMP8 Enhanced Investment in Cyber Security

Option Name	CapEx	Present Value Whole Life Costs* (WLC)	Present Value Whole Life Benefits* (WLB)	Benefit/Cost Ratio	Net Present Value* (=WLB-WLC)
Cyber Security	£10M	£13M	£1,214M	93.91	£1,201M

* pre frontier shift and real price effects, and in 2022/23 price base

As with the analysis for physical security, the CBA is limited by its ability to deal with low probability high consequences events. In this case we have included the consequences of a serious cyber-attack on the service we provide to customers in the 'do nothing' scenario. Such a breach would have serious consequences and as such the proposed protective measures have resulted in a significant benefit.

Whilst this analysis underlines the importance of cyber security. The case for investment is underpinned by governmental requirements rather than CBA analysis.

3.2.2 Quantification of Benefits

Has the company fully considered the carbon impact, natural capital and other benefits that the options can deliver?

Has the impact of the proposed option on the identified need been quantified, including the impact on performance commitments where applicable?

– Ofwat's final methodology for PR24, Appendix 9, A1.1.2c and A1.1.2d

Our approach to benefit assessment is set out in WSH50-IP00 Our Approach to Investment Planning (Section 4.3).

For this investment case option, selection is strongly influenced by set standards and requirements and as such wider benefit assessment has not played a part in option selection.

Table 7 shows the distribution of benefits within the enhancement case for cyber security.

Table 7: Benefits of AMP8 Enhanced Investment in Cyber Security

Scenario	Benefits from AMP8 Spend relative to Baseline			
	Legal Compliance	Security (cyber)	Security (physical)	Total
Preferred	0.1%	90.7%	9.3%	100%

The benefits gained include the avoidance of potential and probable losses associated with cyber-attacks, such as costs of virus or ransomware attack, reputational damage, financial and legal liabilities and loss of productivity resulting from an attack. The benefits from physical security breaches have been assessed more conservatively with lower probability of security failures resulting in lower calculated benefits.

3.2.2.1 Quantifying the Impact on Need and Performance Commitments

By their nature, security measures have no direct measurable impact on the performance commitments.

The security measures will reduce the risk of catastrophic failure due to loss of an asset or an IT/OT system due to a cyber-attack.

These are medium-likelihood, high-consequence events, and do not link through to annual performance targets.

3.2.3 Uncertainties relating to Cost and Benefit Delivery

Have the uncertainties relating to costs and benefit delivery been explored and mitigated? Have flexible, lower risk and modular solutions been assessed – including where forecast option utilisation will be low?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.2e

The Cyber Security options are required to meet a minimum standard for CNI assets.

Cost uncertainty is partially mitigated by use of fixed price managed service contracts, e.g., for SOC provider and Incident Response Retainer.

3.2.4 Involving Customers in Option Selection

Where appropriate, have customer views informed the selection of the proposed solution, and have customers been provided sufficient information to have informed views?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.2h

It is not appropriate to consult with customers on the details of security design options.

We have instead worked closely with the government departments – the National Cyber Security Centre (NCSC) and DWI/Welsh Ministers to confirm the proposed solutions.

3.3 Costing Efficiency

In this section we give details on our approach to costing. Our overarching approach to developing efficient costs is set out WSH50-IP00 Our Approach to Investment Planning (Section 4.10).

3.3.1 Developing a Cost for Security

Is it clear how the company has arrived at its option costs? Is there supporting evidence on the calculations and key assumptions used and why these are appropriate?

Does the company provide third party assurance for the robustness of the cost estimates?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.3a and A1.1.3c

The cyber security costs are based on a continuation of our investment in line with AMP7 and in response to the evolving threat landscape.

We do not anticipate the external threat levels to ease and, indeed, expect we will need to continue investment as attack tactics, techniques and procedures (TTPs) evolve, for example through exploitation of Generative AI and Large Language Models (LLMs).

We have also employed third party consultants to review enhancement cases to provide confidence that the estimates within them are robust, efficient and deliverable.

3.3.2 Benchmarking Our Approach

Is there evidence that the cost estimates are efficient (for example using similar scheme outturn data, industry and/or external cost benchmarking)?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.3b

For cyber security, cost visibility is generally restricted given the secure nature of the work being undertaken, and as such benchmarking is similarly restricted.

3.4 Providing Customer Protection

Are customers protected if the investment is cancelled, delayed or reduced in scope? Does the protection cover all the benefits proposed to be delivered and funded?

– Ofwat’s final methodology for PR24, Appendix 9, A1.1.4a and A1.1.4b

We are not proposing a PCD for cyber security given its relatively low cost and the complexity of measuring outputs.

This area already has strong oversight from UK and Welsh Government.

Oversight of the NIS Regulations is the responsibility of the Welsh Ministers, who have delegated the responsibility to the DWI. It is a requirement that we follow all guidance and advice published by the DWI.

To demonstrate compliance, water companies are required to demonstrate they have achieved the required Sector-Specific Profile (SSP) based on the Cyber Assessment Framework (CAF) by 2025 and that they are work towards meeting the Enhanced CAF (eCAF) by March 2028.

The eCAF is now confirmed in England, with Welsh Government working towards ratification in Wales. Progress against the CAF is tracked through an annual assessment process to DWI.

Compliance failure is dealt with via enforcement actions (which can include formal requests for information, mandated remedial actions, and, potentially, financial penalties).

4. Appendix A

Table 8 shows the total CapEx enhancement costs in AMP 8 for this enhancement case. The Ofwat drivers that this enhancement case maps to are:

- Security - SEMD; enhancement water CapEx (CW3b.121)
- Security - Cyber; enhancement water CapEx (CW3b.124)
- Security - Cyber; enhancement wastewater CapEx (CWW3b.174)

No other enhancement cases contribute to these drivers.

Table 8: TotEx in AMP8 Plan

	Year in AMP8					Total
	1	2	3	4	5	
CW3b.121	£6.489M	£6.396M	£6.393M	£4.191M	£0.000M	£23.469M
CW3b.124	£1.113M	£1.097M	£1.097M	£1.104M	£1.117M	£5.527M
CWW3b.174	£1.114M	£1.097M	£1.097M	£1.104M	£1.117M	£5.529M
Total	£8.716M	£8.590M	£8.587M	£6.398M	£2.234M	£34.525M

** post frontier shift and real price effects, and in 2022/23 price base*

What We Will Deliver:

For the physical security enhancements, this will require upgrades to: Fences, Intruder Alarms, Doors, Window Bar sets, CCTV across 11 sites.

For cyber security, the work will include Extended Detect and Respond (XDR) solutions and Enhanced Security Operations Centre (SOC) Security Information and Event Management (SIEM) capability across Operational Technology (OT) environments.