IT and Telecoms Strategy

WALES&WEST UTILITIES

Contents

Legal Notice

This paper forms part of Wales & West Utilities Limited Regulatory Business Plan. Your attention is specifically drawn to the legal notice relating to the whole of the Business Plan, set out on page 3 of Document 1 of WWU Business Plan Submission. This is applicable in full to this paper, as though set out in full here

Acronym Key	
CAF	Cyber Assessment Framework
Capex	Capital Expenditure
DNCS	Distribution National Control System
ERP	Enterprise Resource Planning
FTE	Full Time Employees
IT	Information Technology
LIDAR	Light Detection and Ranging
NCSC	The National Cyber Security Centre
NOC	Network Operations Centre
OES	Operators of Essential Services
Ofgem	Office for gas and electricity markets
Opex	Operational Expenditure
OT	Operational Technology
PaaS	Platform as a Service
RRP	Regulatory Reporting Pack
SaaS	Software as a Service

1. Overview

At Wales & West Utilities, it's our responsibility to transport gas to homes and businesses in Wales and the South-West of England, through our network of pipes. We don't sell gas. We look after our pipes and assets to keep the gas flowing safely and reliably.

The area we serve is a mixture of cities, towns, villages, and open countryside. While much of our gas network is out of sight and underground, our services are easy to see in the everyday lives of our customers. Whether a safe and reliable gas supply heats a home or business, powers an oven to cook the family meals or warms the water for a nice hot bath, we understand how important it is for our services to be there when our customers need them.

Here are some of our key facts:

We own and maintain over 35,000km of gas pipes
Supplying 2.5 million households and 100,000 businesses
550,000 of homes are on the Gas Suppliers Priority Service Registers
Serving 7.5 million people
Covering North Wales to South Cornwall
There for our customers 24/7, 365 days a year

2. Executive Summary

As we enter RIIO-GD3 we will have completed a major overhaul of our technology estate and achieved what we set out to in our RIIO-GD2 objectives. We will move into the period with a stable foundation of technology systems having reduced our dependency on existing data centres in favour of cloud services and migrated most of our SAP estate from ECC to S/4 HANA (a major step forward in functionality and performance), and upgraded many of our standard legacy systems to the latest available versions.

Through the transformation of cloud technology to serverless and service-based solutions at the forefront of our digitalisation initiatives, we will continue to transform our technology landscape. We will build upon data as a strategic asset to the business, minimising silos and digitising processes. This includes further expansion of the data lake as a standardised and centralised backbone of analytics and reporting which will have been established as part of the data and digitalisation workstream in RIIO-GD2.

Our RIIO-GD3 strategy will further strengthen our technology platform within the business while maintaining the key strength that we will have achieved by the end of RIIO-GD2.

3. Introduction

3.1. Background

In RIIO-GD2, we set out with a clear plan to invest heavily in our legacy application landscapes, infrastructure, and core IT applications. This was driven by the ever-changing technology outlook, rising customer expectations, and a challenging geo-political environment that saw an increased threat of cyber-attacks across the industry. We have made significant progress, including establishing a full cybersecurity team, transforming our ERP and cloud computing capabilities, and moving 43% of our applications to SaaS platforms. Our goal is to have all infrastructure on cloud platforms by 2026.

However, with technology being an ever-evolving challenge, our work during RIIO-GD2 does not mean that we can be complacent in RIIO-GD3. Along with the rest of the world, we see the risk of cyber-attacks becoming ever more likely due to the global landscape. This means we have further work to strengthen our defences and keep our systems resilient and protected from impact. As environmental challenges increase, we will need to support the business to achieve net zero targets by furthering our cloud computing capabilities, which are constantly evolving with more providers offering SaaS solutions. Additionally, there are new licence conditions around data and digitalisation, which require us to establish new capabilities to share our data across the rest of the industry and stakeholder communities. All these points mean that we will need new expertise in these areas, either by bringing in new skills to the business or upskilling our current employees.

Our RIIO-GD3 submission is a higher base allowance than we required in RIIO-GD2, as we are adapting to and meeting new technology challenges and evolving cyber threats. The re-openers mechanism in RIIO-GD2 has allowed us to reach a baseline Cyber Assessment Framework (CAF) profile, and we have already started building towards an enhanced CAF profile. To ensure we stay on track, we significantly increased our headcount in both our cyber and IT departments.

To build our plan for RIIO-GD3, we worked with business partners, stakeholders, and industry leader Gartner Consulting, leveraging their research of trends and hype cycles across utility businesses and peer organisations to give an unbiased view of external factors. The Gartner Hype Cycle is a graphical representation of the lifecycle stages a technology goes through, from the initial development to its commercial availability and adoption, as well as its eventual decline, obsolescence and replacement with new solutions; and is a way for clients to track technology maturity and future potential. Gartner have validated that our IT & Telecoms capital programme is towards the lower end of the expected range based on their benchmark. Most of our large value investment initiatives are in range or lower than the Gartner Low bracket, with the exception of Digital Twin. This prudently reflects the inherent uncertainty in this initiative at this time, with funding only allocated for a 'discovery' phase aimed at generating greater cost clarity potentially to be included in a GD3 re-opener. Our increased Opex spend compared to GD2 reflects our greater use of subscription services and use of outsourced service providers.

Most importantly, we have built this plan in full collaboration with our internal and external stakeholders to ensure we meet their expectations and deliver an IT and Telecoms plan that fully supports their ambitions during RIIO-GD3.

3.2. Current State

In RIIO-GD2 we focused on 3 main areas;

1. **Modernisation and Efficiency.** By replacing legacy applications with industry-leading solutions, we are enhancing efficiency, customer service, safety, and network performance. This included modernising core IT applications and investing in IT infrastructure to support these initiatives.

2. **Investment and Projects.** We invested £41m across approximately 46 key projects during the RIIO-GD2 period. These projects improved reliability, increased capacity, and leveraged cloud technology for scale and efficiency.

3. **Strategic Objectives.** The objective was to simplify and modernise applications, reducing technical debt, and enabling a predictable, efficient cost base. Key objectives included consolidating IT applications, promoting agility, and implementing applications that can be integrated with other systems as a precursor to digitalisation.

In RIIO-GD2 our allowances in these areas increased significantly through the re-openers process, reflecting how we are adapting to technology advancements across the industry and an ever-evolving landscape of cyber threat. In response to this increasing cyber threat, we made changes during the period to achieve a Base CAF profile and start building towards an Enhanced CAF profile. This means we exit RIIO-GD2 and enter RIIO-GD3 with a larger and more capable team at a necessarily higher running cost than at the beginning of RIIO-GD2.

In RIIO-GD2 we have achieved the following outcomes:

SAP S/4 Hana	Implemented Finance and HR modules
Cloud adoption	> 43% of applications now SaaS
Resilience improvements	Major programme to address technical debt
Team capability	Additional resources and expertise introduced to the Target Operating Model to meet demand
Cyber team established	Skills and expertise expanded to the Target Operating Model to achieve CAF profile
Ofgem relationship	Closer working relationship
Service stability	Reduced rolling average of critical incident
Audit	Disaster Recovery, Governance, IT controls overhauled
Contract performance	Contract review and gap analysis complete
Application discovery	Shadow IT and non lifecycle applications identified
Business relationship	Relationship managers in place to lead on business Return on Investment (ROI)
Re-openers	Doubled allowances through re-opener mechanism to deliver security programmes for CAF Compliance
Physical capability	Established a dedicated physical security team and policy reviews

We have responded to an increasingly unstable geopolitical landscape with increases in both cost of living and cyber-threat levels.

The challenge of sustainability and supporting net zero has also been part of our work, establishing cloud computing and energy efficient solutions. As these circumstances continue; in our RIIO-GD3 plan we place greater demand on rapid change for increased security, sustainability and digitalisation.

Rising cyber threat leads to rising costs during RIIO-GD3

Overall RIIO-GD3 cost increases are due to several factors. These include requirements from Operators of Essential Services (OES) for regulated and enhanced cyber security controls. In addition, a greater risk exposure to WWU has been forecast, due to the rising sophistication levels of attackers and an increase in global threats.

3.3. Target State

Our commitment to providing safe and reliable services to our stakeholders has led to us establishing principles and standards that we hold ourselves accountable to. It is these principles which guide us to our target state.

As we operate throughout RIIO-GD3, our enterprise technology will support the efficient delivery of digital services to our workforce and stakeholders. We will be compliant with all our principles; policies; and standards; with a robust, reliable technology footprint that is predominantly cloud-based and highly resilient. We will have completed rationalisation of our application portfolio and re-architected many services to cloud-based solutions, delivered online. Our Finance systems will have merged into a single Enterprise Resource Planning system and our workforce management applications will have consolidated to a simpler to operate experience for all our field teams providing easy and accurate data capture of all our digitalisation needs. We will be openly sharing catalogued data sets with third parties and preparing our organisation for the future energy needs of the region.

3.4. Scope

The scope of the strategy covers both Information Technology and Operational Technology, including their supporting data and voice communications networks.

Areas in scope are as follows:

Lifecycle Management - Establish that the hardware, software, and network resources necessary for operations are maintained, updated, and scalable to meet stakeholder needs.

Technology Management - Oversee the creation, deployment, and maintenance of technology solutions that support new or enhanced business processes and goals.

Data Management - Implement practices for data storage, security, and analytics to enable informed decision-making and protect sensitive information.

Security - Establish processes and procedures to safeguard the organisation's assets against cyber threats and ensure compliance with regulatory requirements.

Innovation and Emerging Technologies - Explore and integrate new technologies that can drive improvement and operational efficiency.

Governance and Policy - Define the rules, policies, and procedures for IT operations to ensure consistency, reliability, and alignment with business objectives.

Contract Management - Manage relationships with external technology providers to optimise service delivery and cost efficiency.

Skills & Development - Developing IT staff skills and knowledge to keep pace with technological advancements and improve overall performance.

These areas confirm that our strategy supports our overall organisational objectives and will provide sustainable and reliable operations.

3.5. Drivers

The primary drivers of our RIIO-GD3 plan are to deliver a safe and reliable service to our stakeholders in an efficient and cost-effective manner. The four pillars that drive our strategy are:

Resilience Throughout RIIO-GD3 we will continue to maintain our technology landscape to the standards and principles we set in RIIO-GD2 securing well supported technology that operates safely and reliably.	**Digitalisation** Rationalising our technology landscape is crucial to support an efficient, defined catalogue across our systems and processes.
Customer Service Our technology must be reliable and efficient; and we must be easy and accessible to do business with. Our solution design cycle focusses on accessibility alongside security and reliability	**Sustainability** While technology is essential to our operations; we can reduce our carbon footprint by using cloud providers that are committed to net zero targets, and by considering energy efficient products

4. Key Outcomes

The following list details our intended overarching outcome areas for RIIO-GD3, with the actions we will take to achieve them.

Reliable and resilient services

- Align the IT strategy and roadmap with our organisational objectives.
- Maintain supported lifecycle of technology solutions to N-2 versions.
- Design and deliver solutions to meet standards and legislation.
- Manage the performance and delivery of service providers.
- Identify new opportunities for technological improvement.

IT and Telecoms

- Design and deliver technology aligned to the business objectives and regulatory outputs.
- Lifecycle maintenance for all technology clear roadmap to stay in support.
- Compliance with all relevant legislation and license conditions e.g. Data & Digitalisation.

Operational

- Improve agility and efficiency through well designed solutions.
- Provide resilient & cyber-secure IT services.
- Adopt a Cloud-first strategy for lifecycle management & IT Disaster Recovery.
- Protect and increase the value of organisational data.
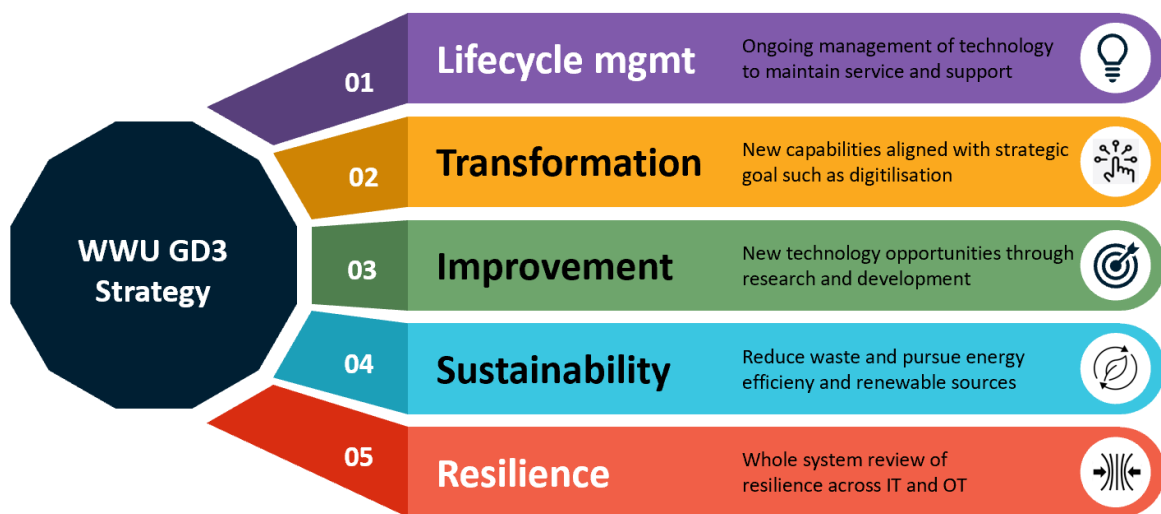- Manage costs efficiently and minimise duplication.

Technology

- Define the overarching goals and objectives of the IT and Telecoms Strategy.
- Outline key initiatives and strategies proposed to achieve the defined objectives.

5. Business Context

5.1. External Factors

	External Factors to consider	Factors affected within our industry	Importance to organisation
Economic	Inflation, cost of living, market demand	Employee attrition; skills retention	Staff retention
Environmental	Climate change, biodiversity, natural resources; sustainability	Energy consumption, supply chain sustainability	Net zero commitments, efficiency.
Geopolitical	Threat landscape and supply chain instability	Policy and regulation	Governance and audit overheads
Societal	Societal polarisation,	Corporate responsibility	Workforce and talent development, retention
Technology	Renewables, Digitalisation	Artificial intelligence	Automation; information management
Legislation	Environmental, HSE, Data protection, Resilience	NIS2, Utility procurement	General Data Protection Regulations, Network Information Systems, Health & Safety Executive, Public Utility Procurement Regulations

6. Strategic Themes

		Description	
01	**Lifecycle mgmt**	Ongoing management of technology to maintain service and support	
02	**Transformation**	New capabilities aligned with strategic goal such as digitilisation	
03	**Improvement**	New technology opportunities through research and development	
04	**Sustainability**	Reduce waste and pursue energy efficieny and renewable sources	
05	**Resilience**	Whole system review of resilience across IT and OT	

WWU GD3 Strategy

6.1. Lifecycle management

This category is a crucial foundation to ensure a stable environment in which business activities are supported, and we are prepared to deliver the future change required for net zero. This needs certainty that existing technology is current, well maintained and supportable. It includes application consolidation, re-platforming, lifecycle maintenance, updates, and process monitoring to reduce downtime and improve performance and efficiency. We will continue to invest in the maintenance and management of solutions that are required for the future, and work towards the replacement or retirement of those that are not. The assessment of the current technology estate has considered the view of process and system owners of the relative functional and technical fit. This is with a view to determining the most efficient Total Cost of Ownership in the plan, and a TIME based classification along the lines of Tolerate, Invest, Migrate, or Eliminate.

6.2. Transformation

Building on our foundational projects; transformative change programmes will deliver new functionality and capability into the organisation aligned with our strategic goals. Much of this is driven by key strategic objectives such as net zero targets, digitalisation best practices, and resilience. Improving outcomes for our stakeholders is also key, in the areas of safety, environment, customer service, asset management and HR. We will deliver a programme of work sponsored by business directorate specific needs. We encourage a collaborative approach and use technology to boost productivity and data quality.

6.3. Continuous improvement

In addition to enabling business transformation through technology adoption we will seek opportunities to lead in areas of new and emerging technology. This involves research and development; proof of concept and trial of new technologies; testing innovative projects and fostering a culture of continuous improvement. The focus is on staying ahead as a digital business and being leaders in emerging technology trends where they support business ambitions. Together these initiatives are designed to create a robust, flexible, and forward-looking IT department that will lead the organisation into a new phase of digital transformation.

6.4. Sustainability

Within IT we will reduce waste, procure energy efficient systems and dispose of equipment in as sustainable a manner as we can. Our cloud migration will use a more efficient data centre with commitments to reducing carbon and renewable energy. Through our Environmental Action Plan (EAP) we will leverage technology to drive sustainability through initiatives that include the following

1. **Advanced Methane Detection** - Implementation of advanced methane detection technology to report real-time emissions, coupled with a sophisticated analytics platform to improve targeting of mains replacement and leak repair.
2. **Digital Transformation and Paper Reduction** - Efforts to digitise depot site folders, introduce apps for drivers, and review business processes to reduce paper consumption and eliminate the need for printing.
3. **Waste Management and Recycling** - Development of waste management apps, online dashboards, and continuous improvement initiatives to increase recycling and manage waste effectively.
4. **Environmental Performance Monitoring** - In-contract monitoring of environmental performance of contractors and suppliers to ensure they meet environmental metrics and contract requirements.
5. **GIS Land Holdings Database** - Creation of a Geographical Information Systems land holdings database using LiDAR (a remote sensing method using light detection) and satellite data to classify land holdings according to ecological status, risk, and opportunity for community use or asset transfer.

6.5. Resilience

Our objective as an operator of essential services is to ensure the continuous and reliable delivery of critical functions and services, even in the face of disruptions. This will be achieved through the following activities:

- **Continuous Risk Assessment** - Identifying potential threats and vulnerabilities that could impact operations.
- **Preparedness** - Developing and implementing continuity and disaster recovery plans to mitigate identified risks.
- **Response** - Establishing protocols for rapid and effective reaction to incidents to minimise service disruption.
- **Recovery capability** - Sufficient plans and skilled workforce to ensure quick restoration of services to normal operation after a disruption.
- **Adaptability** - Continuously improving and updating resilience measures based on lessons learned from past incidents and emerging threats.

7. Workstreams

We have set out key workstreams, each of which are indicative of our levels of ambition from must-do to futuristic thinking. Each category contains key initiatives which we will deliver in RIIO-GD3. The initiatives in each of these categories are designed to create a robust, flexible, and forward-looking IT landscape that will lead the organisation into a new phase of digital transformation.

7.1. Alignment with Business Objectives

This workstream is to align IT and Cybersecurity best practices and roadmap with our organisational strategic goals. We will deliver a programme of change sponsored by workstream and directorate specific needs; we encourage a collaborative approach; and use technology to boost productivity and data quality. Our joint goal is to become a valued delivery partner that supports and enables business goals through good technology.

Target: Compliance with principles, policies, standards

7.2. Technology Innovation:

The strategy stresses the importance of continuous improvement and exploring opportunities to lead in areas of new technologies. This involves research and development, proof of concept and trial of new technologies, testing innovative projects, and fostering a culture of continuous improvement. The focus is on staying ahead as a digital business and being leaders in emerging technology trends where they support business ambitions.

Target: Efficiency gains and value returned to stakeholders

7.3. Cloud Migration

In 2019 we implemented the infrastructure to support our SAP (Systems Applications and Products in data processing) solution for Finance and HR in Microsoft Azure. Our SAP system was the first to be built in our Azure environment and since then more new services have been deployed as a cloud-first solution. By the end of RIIO-GD2 we will have completed our migration of IT workloads to the cloud in preparation for exit from our on-premises data centres which have been owned and operated by a third party (SCC) since 2012. The remaining Operational Technology workloads will be migrated by Dec 2027. Microsoft Azure data centres are built to a standard that we could never hope to achieve through investment in our own equivalent. Each Microsoft Azure region invests around $4bn in establishing services offering levels of resilience unachievable on a small scale. These cloud services afford us a greater level of resilience and scalability than we could achieve on-premises and therefore form a pivotal part of our disaster recovery improvement plan.

7.4. Data and digitalisation

Our Wales & West Utilities Digitalisation Strategy sets out four goals for transformation:

1. Become a digital utility by re-thinking the business, challenging existing business processes, and modernisation of technology to enable the efficient exchange of information between all areas of our business, our customers, and the outside world.

2. To enable our workforce to operate as a modern digital workforce where we can operate, communicate, plus organise tasks and events seamlessly.

3. To enable our customers to engage with us in the most appropriate manner via a multi-channel experience that is simple and efficient.

4. Provide a digital approach for the integration of technologies for the real-time management of a connected gas network that provides an efficient customer experience.

This will result in changes in the way we catalogue, govern and consume data among our stakeholders as the demand for data continues. Our RIIO-GD2 commitment from the re-opener funding continues into RIIO-GD3 and we will carry the target operating model for data governance and open data sharing into RIIO-GD3.

7.5. Cyber Security

The Cyber Security Strategy outlines Wales and West Utilities' strategic approach to improving cyber resilience during the RIIO-3 period (2026-2031). It is part of a suite of documents that make up WWU's RIIO-3 business plan for Cyber Security and is intrinsically linked to the IT and Telecoms strategy. IT sets out 5 main themes as follows:

1. Standards and Certification: The primary focus for 2026-2027 is to achieve full compliance with the NCSC CAF enhanced profile and attain ISO27001 certification.

2. Continuous Improvement: For the period 2028-2031, the strategy emphasises continuous improvement processes, anticipating new compliance targets and technical advancements such as zero trust technologies and artificial intelligence.

3. Robust Management: The program will be robustly managed, with ongoing tracking of progress against plans, risk reduction, and alignment with the CAF enhanced profile.

4. Building Resilience: The strategy aims to continue to build resilience against a diverse and complex threat landscape, including ransomware, state actors, and extremist groups.

5. Organisational Culture: Developing an organisational culture that recognises security as a core corporate value, ensuring that security is everyone's responsibility.

8. Implementation Plan

8.1. Roadmap to deliver

Lifecycle management - Having completed the RIIO-GD2 goals we will carry on the extensive work we have done, by ensuring that all our systems stay in the support and are upgraded to version N-2 as set out in our architectural principles.

Value for Money - We have planned our budgets to be set against projects of varying difficulty and we will flex resources via our partner network as required to achieve these goals and deliver these projects.

Business support - We will have a greater emphasis on supporting the business with their goals and objectives that require technology to deliver. We have engaged with colleagues throughout WWU during the planning process, and we will continue this within RIIO-GD3 as required. Many of the projects we have set out in our Capex plan align directly to business sponsored initiatives, delivering well architected solutions for business units to be able to deliver on their own outcomes.

Consolidate partner network - As we approach RIIO-GD3, although our technology stack may be more complex with highly resilient cloud services, our complex supply chain will reduce as we consolidate our technology footprint and partner network. While re-tendering contracts we will consolidate and streamline our support model via a smaller partner network; and a stronger in-house team for agile development, modern workplace support and operational technology management.

Consolidate Application Stack - In line with our architectural principles we will continue to avoid duplication and reduce our total number of applications during the RIIO-GD3 period. This may involve re-architecting, replacing and retiring some applications as we select replacements with an improved functional and technical fit. This may result in wider portfolio for IT/OT as we adopt solutions currently developed outside of IT.

S4 - As part of our delivery plan SAP S4 will play a huge role in key business processes as it does today. We will continue to leverage this platform and services that we already use to enhance business performance; by consolidating our S4 platforms hosted in Microsoft Azure and exploiting SAP functionality within the platform wherever possible.

8.2. Resource

Throughput RIIO-GD2 we have expanded our target operating model (TOM) within the IT Team to deliver against the operational demands due to the drivers we identified. This expansion has been supported by our regulator through the re-opener mechanism for allowances and our strategy sees us carry forward this new TOM into RIIO-GD3 at the current levels of resource. This is crucial to be able to continue to meet the demand of rapid change required because of external factors such as security and resilience, but also new capabilities such as digitalisation.

8.3. Risk Management

We have developed the maturity of our risk management processes throughout RIIO-GD2. The addition of a dedicated risk management function within IT supports the alignment of technology deployment with measured and efficient risk reduction.

8.4. Change Management

Our approach to change management in RIIO-GD3 will modernise as we move to cloud-native environments and realise agility, automation, and continuous improvement. We will use automation tools to implement Infrastructure as Code (IaC), enabling consistent and reproducible environment setups. We will operate Continuous Integration and Continuous Deployment (CI/CD) pipelines for frequent, reliable updates, minimising downtime. A network operations centre will introduce monitoring and visibility of critical operations, providing real-time insights and rapid issue resolution. Security and compliance are already embedded into the development lifecycle, ensuring robust protection against vulnerabilities and this will continue. This strategy fosters resilience and scalability while allowing innovation and agility in cloud-native ecosystems.

9. Governance

9.1. Digital Technology Group

The digital technology group chaired by the Chief Information Officer CIO and attended by all principal senior managers across directorates will oversee the execution of the IT and Telecoms strategy.

The group is responsible for:

- Business Case review, prioritisation and approval to proceed.

- Providing the forum with all appropriate actions noted and prioritised to underpin the success of IT Programmes of work.

- Overseeing business and financial risks associated with the programmes.

9.2. Architecture Review Board

The board is responsible for design assurance of all technology change within the organisation and is attended by representatives from Architecture, Service and Security.

9.3. Programme Governance

Project and programme governance follows a gated methodology overseen by the Project Management Office with all project workstream decisions managed by a project board attended by the project sponsor.

9.4. Stakeholder Engagement:

To prepare the IT Telecoms plan, we have worked closely with our colleagues from every directorate and every application owner to gather technology requirements for RIIO-GD3 based upon their own workstream plans. All initiatives across these workstreams areas have each in turn carried out their own external stakeholder engagement. The validity of which therefore carries through into the IT and Telecoms plan. All initiatives have been identified by assessing business objectives and key market trends across the industry, which have also been subject to public engagement. As mentioned earlier in the strategy, we commissioned Gartner to review and assure the plan for effectiveness and cost efficiency.

10. Financial Overview

10.1. Headlines

- Our RIIO-GD2 allowance for IT and Telecoms more than doubled through re-openers during the period.

- We expect this to continue until the end of RIIO-GD3, driven by legislation and license conditions aimed at improving UK resilience to current geopolitical threats.

- There has been a shift to Opex due to the need for cloud technology subscription-based services.

10.2. Legislative drivers

- GDPR – General Data Protection Regulations

- NIS – Network Information Systems

- D&D - Data & Digitalisation

10.3. Cost drivers

- Increased IT & Cyber headcount approved through re-openers

- IT computer workloads migrated to cloud in RIIO-GD2; increase in Cloud platform services and growth in subscription services, shift from Capex to Opex (SaaS, Data migration to Cloud)

- Increased adoption of digital processes and a larger application estate.

- Introduction of a new capability, Network Operations Centre (NOC) for proactive 24/7/365 capability.

- Ongoing operational costs of RIIO-GD2 reopeners continues into RIIO-GD3 forecast, e.g. Data & Digitalisation £0.5m for consumption charges.

- Our assumption is reopeners will still be a necessary mechanism in RIIO-GD3 for initiatives that continue to have a level of uncertainty.

- Ongoing lifecycle management to tighter timescales for a cloud environment.

10.4. New factors in RIIO-GD3

- In-house 'DevOps' application development capacity for business-led requirements.

- SAP ECC/S4 consolidation to follow the RIIO-GD2 Finance and HR releases.

- Application modernisation and transformation to Platform as a Service (PaaS).

- Application consolidation, balanced by application expansion as we adopt new digital tools (e.g. Cyber, IT, Asset, Customer, Future of Energy (FoE), Data & Digitalisation, AI, Streetworks, H&S).

- Business-led functional enhancements: HR, Finance, Asset Management, Customer relationship management, Supply chain, Environmental, Fleet management, Operations, Facilities, and Innovation.

- New capabilities: RRP automation, Data & Digitalisation, Hydrogen blending.

10.5. Financial Summary

The increase in Opex reflects the move away from on-premises IT solutions towards more SaaS, consumption-based IT. It also recognises the additional people required to deliver against increasing requirements to invest and maintain the security of our IT systems. This is a priority as we exit RIIO-GD2 and is the basis of requirements within our RIIO-GD2 reopener submissions which we must continue to operate in RIIO-GD3.

This also includes Cyber and Physical Security Opex, continuation of the pathway set out in our submitted RIIO-GD2 re-openers; detailing the factors required to keep our network safe and resilient, and to meet and maintain compliance with our obligations under the current Network and Information Systems (NIS) and Cyber Assessment Framework (CAF). The costs included in our plan achieve a CAF Enhanced Profile by 31 December 2027; further improvements or requirements will require use of the re-opener mechanisms where appropriate.

11. Risk Management

11.1. Our approach to risk reduction

Achieving risk reduction involves a multi-faceted approach. Implementing rigorous risk management processes and mitigation projects along with regular maintenance schedules confirms the reliability and safety of systems. Investing in advanced technologies, such as highly available and real-time monitoring systems, helps in early detection and mitigation of potential issues. We invest in our people and training programs to ensure they have the skills and awareness necessary to respond to emergencies. Fostering a culture of continuous improvement and compliance with regulatory standards creates long-term operational resilience and safety.

11.2. Operational Telecoms 24x7

Communications networks, both voice and data are critical services that we rely on for monitoring, managing and executing work across our gas network. We have already replaced our Public Switched Telephone Network (PSTN) services as a result of Openreach withdrawing these services from the wholesale market. As we approach RIIO-GD3 we will have completed re-tender events to establish contracts for next generation voice and data across our portfolio of services. Due to the complexity of any potential migrations, the implementation effort will run into RIIO-GD3, but we are likely to see the adoption of Software Defined Wide Area Network (SD-WAN) alongside fibre and satellite communications for full diversity. We are working with the strategic telecoms group on what a utility focused low power, long range telemetry network may look like for increased independence and resilience.

11.3. Operational efficiency

As technology is a supporting service to the operations teams, we aim to simplify the application landscape, work management and data capture processes across the operations teams. Multiple work management applications will be consolidated into a single field application. Handheld mobile devices will be reduced to remove the overhead of carrying laptops, phones and iPads for different processes/applications. Single sign-on and role-based access will further simplify the operational experience while also increasing resilience against external threats.

11.4. Operational resilience

We ensure continuous service of data and voice network services through diversity of services and supply chain. At a time when most organisations will be converging data and voice for efficiency and savings; we must continue to maintain resilient and diverse connectivity for telemetry and control systems, with robust continuity arrangements so that we can safely operate our Gas network manually if absolutely necessary.

11.5. Risk Profile

Risk Categories
- Resilience
- Operational
- Compliance
- Governance
- Information
- Strategic
- Environmental
- Financial

Short term

1st	Lifecycle management
2nd	Access management
3rd	Process & policy
4th	Cyber security
5th	Disaster recovery
6th	Asset management
7th	System availability
8th	Supply chain
9th	Infrastructure
10th	Resourcing

Long term

1st	Sustainability
2nd	Supply chain
3rd	Data growth
4th	Technology (AI)
5th	Resourcing
6th	Cyber security
7th	Asset management
8th	System availability
9th	Lifecycle management
10th	Infrastructure

12. Conclusion

Our IT and Telecoms Strategy is designed to help us deliver an enhanced service for our stakeholders and will ensure a reliable and resilient organisation now and in the future. One of the key areas of focus is the continuous investment in modern technology to ensure we keep pace not only with the expectations of our workforce and stakeholders, to provide accessible and efficient services but also with the need to remain resilient against an existential threat as a result of the geo-political landscape. As we replace our older systems we will leverage cloud technology, changing the balance of Capex to Opex and at the same time as improving the sustainability and resilience of our organisation.

We will incorporate oversight of operational technology into the IT and Telecoms strategy ensuring investment plans and maintenance programs are aligned, delivering to the high standards expected of us.

We will ensure our business processes and service delivery continue to provide efficient and effective services by using innovative, automated and integrated IT solutions.

This will help us secure our operations, increase the value of our data, deliver sustainable value for our stakeholders, and satisfy the changing needs and expectations of our customers and workforce.

Our focus on resilience of infrastructure and data assets is the backbone of our strategy and through continued adoption of best practices and industry standards for security and risk management we will minimise any impact to our stakeholders. It is important we protect our information and systems from cyber threats, follow relevant regulations and policies, and recover quickly from any incidents or disruptions.

It is also important that we can support our staff and stakeholders to become more productive and collaborative by giving them access to modern and user-friendly technology services and platforms. This will help us enhance our communication, coordination, and cooperation across different teams, departments, and locations, and to tap into the collective knowledge and expertise of our staff and stakeholders.

We will foster a culture of innovation and collaboration across our organisation by investing in skills development and knowledge sharing. This will help us keep up with the latest IT developments; encouraging our workforce and stakeholders to suggest and adopt new ideas and solutions that will improve our organisational performance and services.

Our IT vision is aligned with the objectives of our organisational values and priorities, and we will continue to regularly monitor and review the relationship. This will ensure our IT roadmap continues to support our organisational objectives, and that we are able to deliver strategic goals.

These outcomes and benefits will help us fulfil our mission and vision, delivering value to our stakeholders. Our IT and Telecoms Strategy is a roadmap for achieving these goals and ensuring our IT function is a strategic enabler and technology partner of choice for our wider organisation.