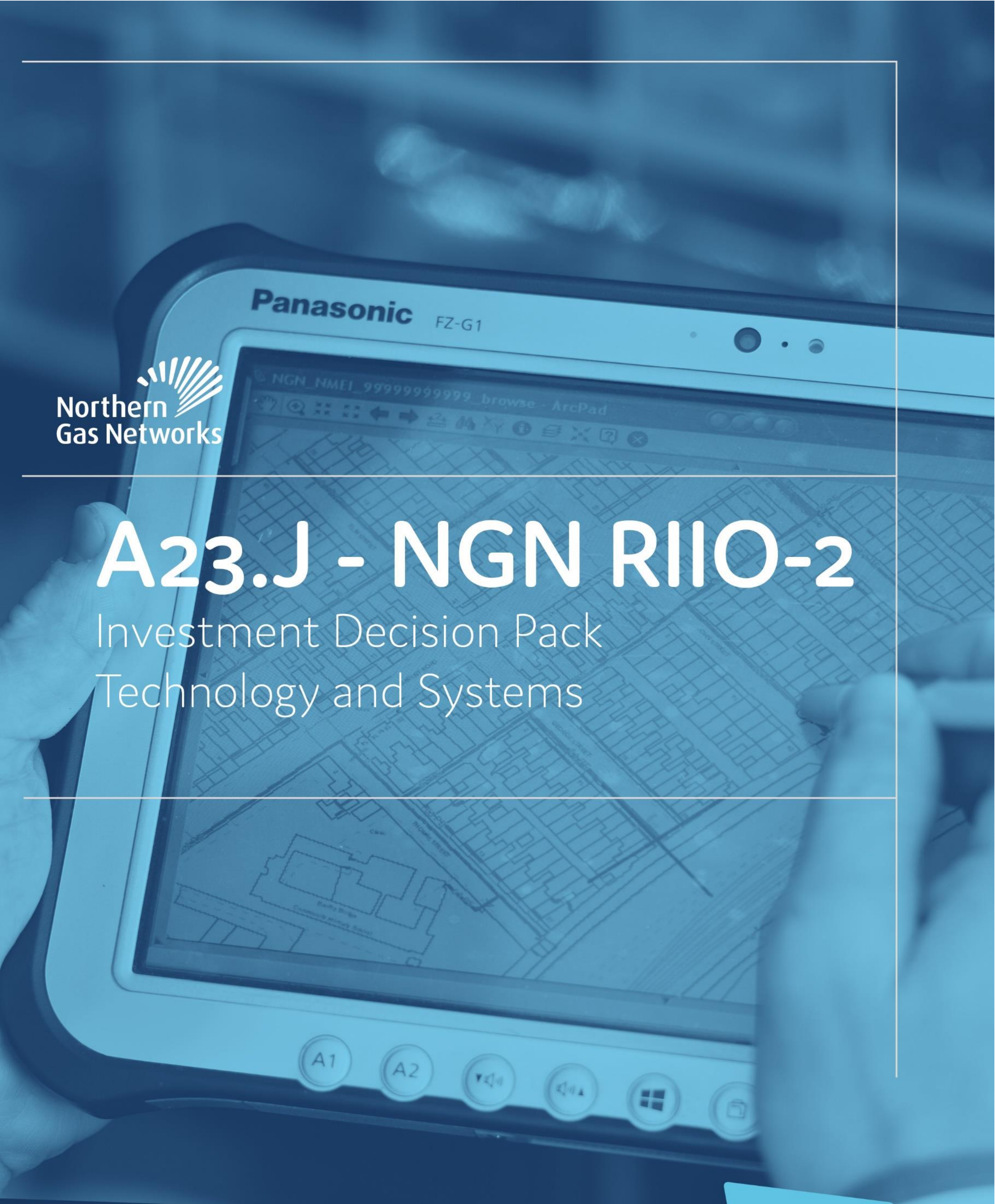


Northern Gas Networks

A23.J - NGN RIIO-2

Investment Decision Pack
Technology and Systems

we are the network

1. Table of Contents

2. Introduction

This Engineering Justification paper outlines the process we have undertaken to determine our capital programme for investment in our Technology & Systems during RIIO-2. We have categorised investments into five areas where there is commonality and shared benefits. These are:

- Devices and hardware
- Network
- Software
- Innovation
- Cyber Security

Each category above will have its own Cost Benefit Analysis (CBA) which will consider different options and be compared to a baseline position to determine the most efficient solution providing the greatest benefit for our employees and customers. Network investment is below Ofgem's materiality threshold and so do not form part of our Cost Benefit Analysis.

3. Equipment Summary

Devices and hardware

This category includes the following equipment and operating systems:

- **Desktop computers** – used by our staff who need a more powerful machine for their role
- **Laptops** – used by our staff for their day to day activities
- **Tablets** – used by our operational staff to access emails and information when out of the office, and capture business critical data at source.
- **Mobile phones** – used by our staff to communicate with colleagues, public and other businesses
- **Monitors** – to enable a larger screen when using laptops in our offices
- **Large screen TV's** – to share important information with colleagues in our offices and depots
- **Microsoft Windows upgrades** – an operating system used on desktops, laptops and servers
- **Cloud infrastructure** – includes public cloud infrastructure, backup and restore capabilities

Network

This category includes the following networks:

- **Wide Area Network (WAN**) – a communications network which spans a large geographical area to connect different parts of our business such as cloud services, offices and depots
- **Local Area Network (LAN)** – a smaller communications network which connects computers within a limited area such as one office block
- **WIFI** – a wireless networking technology that uses radio waves to provide high speed internet and network connections
- **Landline telephony** – a telephone with a physical line connection to a telecommunications network
- **Telemetry network** – a satellite telemetry system which transmits information from our gas sites to our control centre to allow 24/7 monitoring

Software

This category includes the following systems and applications:

- **SAP S/4 HANA** – an Enterprise Resource Planning tool and digital platform that supports our work, asset management and business activities
- **Geographic Information System (GIS)** – a mapping system which stores and analyses geospatial data on our gas distribution network
- **Mobile Data Capture Applications** – mobile applications used by our operatives to capture field data in forms and reports
- **Supervisory Control and Data Acquisition (SCADA)** – a control system used for real time process management of our gas network
- **Other Applications** – includes various applications that support our business processes e.g. Falcon, Synergy, Insight and Lotus Notes

Innovation

This category includes the following:

- **Internet of Things (IoT)** – sensors embedded in assets and equipment to create smart networks where data is collected and transferred over the internet
- **Wearable Technology** – technology worn by our operatives to record their health and safety and performance
- **Virtual Reality –** a safe and realistic virtual training environment in which our operatives can learn the skills required to work on our gas assets
- **Digital Twins** – a digital replica of our gas assets allows our project managers to understand the design and build process of construction projects and our operatives to gain a virtual training and testing environment
- **Process Optimisation and Automation**- to support further efficiencies in our support process by building on the capabilities delivered through S4 HANA
- **Augmented Reality** – to allow our operatives to see critical information through a visual display such as the location of gas and other utility assets

Cyber Security

This category includes the following:

- **Identity and Access Management (IAM)** – allows administrators to control user access to critical information within our organisation
- **Information Security Risk Management (ISRM)** – is a process of managing and reporting security risks associated with business data, intellectual property and physical assets with the aim of identifying, assessing and treating risks and vulnerabilities in accordance with our company's overall risk tolerance
- **Information Security Training, Awareness and Communication** – includes electronic and live information sharing forums which serves to inform employees of their responsibilities for protecting information in their care
- **Network and System Security Architecture** – a tiered network architecture based on the data, business criticality and function that applies appropriate controls to manage the risks at each level
- **Cryptography** – a process by which data is converted into a format that is unreadable for an unauthorised user thus protecting it from misuse

- **System Acquisition, Development and Maintenance** – implementation of Information Security requirements to secure application services and transactions and to secure development and testing practices to review and address security risks before, during and after system changes
- **Secure Communications** – the controls and safeguards necessary to ensure networks are managed adequately, with appropriate segregations and information transfer and security of electronic messaging
- **Asset Management** – the secure management of the physical and data components of Information Systems throughout their lifecycle from acquisition to disposal
- **Operation Continuity and Disaster Recovery** – ensures critical systems are always operational and available, a disaster recovery plan and implementation strategy minimises the effects of unplanned incidents
- **Supplier Relationships** – protection of our assets that are accessible by suppliers through addressing security risks within supplier agreements

4. Problem Statement

Why are we doing this work and what happens if we do nothing?

Device and hardware – Laptops, desktop computers, tablets and mobile phones are critical hardware equipment that our colleagues use daily to undertake their work activities. Without this equipment tasks would either become much more time consuming or impossible to undertake, but with them they provide our workforce greater mobility and localised field data capture. The operating systems these devices use is just as important to the efficiency and security of the device.

Hardware has a relatively short life cycle as planned obsolescence and technological progress leads to outdated and inefficient equipment. Software updates are vital if we want to remain on a secure platform, take advantage of new features and remain supported and compatible. Without investment in RIIO-2 we would be increasing the risk of cyber-attacks resulting in increased employee downtime and the possibility of GDPCR and NIS fines.

Network – Communication networks, wireless networking and our satellite telemetry system enables different parts of our business to communicate with each other which is essential for the efficient running and operation of our gas network and business services. Without these communication networks in place, transfer of data and information would become more difficult and time consuming leading to a slower response to network issues and increasing health and safety, customer and environmental risks.

Software – During RIIO-1 we have replaced our core system, SAP ECC, with the new SAP S/4 HANA Enterprise Resource Planning tool and digital platform, which, along with reorganising our business, this business transformation, will enable us to become more agile with a smart technology approach to back office and operational support. In RIIO-2 we want to make sure we seize the opportunities and benefits that a transition to SAP HANA offers such as real time access to business information, greater mobile working and predictive analytics. We will invest in SAP HANA technologies to continually improve our business processes and deliver technologies that drives innovation, operational efficiencies and simplification of applications and will provide a platform for automation and predictive analytics by capturing all data and work in the SAP system. In addition, we will ensure enhanced security through the latest supported updates and patches.

Our SCADA system which is used for the real time process management of our gas network will be coming to the end of its life and will be replaced with emergent technology to provide more wealth of features, simplifying support and improved security. We also plan to upgrade our GIS mapping software and other applications to facilitate simpler integration with SAP, provide a wider range of features that will simplify the system and improve security through latest supported software. Without these investments in RIIO-2 we would be increasing security risks and the chance of incurring a fine or penalty nor non-compliance. In addition, we would not be maximising the opportunities available to us that a large-scale SAP replacement, like what we have delivered in RIIO-1, offers in terms of increased productivity, improved business processes and better data management.

Innovation – We are committed to realising the benefits from an ever-evolving technology landscape and plan to invest in technology and system innovation such as IoT technology and augmented reality to allow greater real-time monitoring and display of assets across our network to provide a 360-degree view of asset performance and facilitate better decision making that improves operational efficiency, reduces risk and saves our customers money. We also want to improve our colleague's safety through wearable technology and provide a more immersive learning and development environment through Virtual Reality training. If we did not invest in innovation in RIIO-2 we would miss out on the opportunities that new and cleaver ideas can bring to the work place, the improvements they can make to safety and reliability and the efficiencies they can deliver in time and cost.

Cyber Security – We are acutely aware of the threats facing organisations such as ourselves relating to cyber security and will invest in projects to make our systems, networks and data more secure. We will upgrade our Identity Access Management system to control user access to critical information and develop an Information Security Risk Management programme and tiered Network and System Security Architecture to protect our business data and intellectual property. We will manage information and data from acquisition to disposal and have in place Operational Continuity and Disaster Recovery systems to ensure we are always operational and to minimise the effects of unplanned incidents. Investment in cyber security in RIIO-2 will enable us to proactively manage risks to our systems and reduce the number of security incidents. As viruses and hacks become more sophisticated, so does the requirement for our security systems, and through continued investment we can ensure we have the necessary controls in place to protect our assets and data. Without investment in this area, we would likely experience more cyber-attacks detrimentally impacting our business and our assets. We would likely see an increased risk of data breeches and fines due to non-compliance with UK regulations.

What is the outcome that we want to achieve?

The strategic objectives that drive our approach to technology operations are:

- **System availability** – we aim to operate all systems to a minimum availability level of 99.95%, with a recovery time objective (RTO) of 8 hours and a recovery point objective (RPO) of 24 hours.
- **Supported versions** – we aim to operate applications and operating as close as possible to the most recently released version, with a target of being no later than n+1 as the version in use.
- **Cost effective and sustainable** – We aim to operate IT systems and support in the most cost-effective way, through robust challenge to our supply chain and making the best use of cloud technologies. In doing this we will work to reduce our carbon footprint of our technology through the purchasing of efficient devices and aiming greater use of the cloud.

The strategic objectives that drive our approach to technology and improvement are:

- **Information at the heart of decisions** – We aim to place data and information at the heart of how we innovate, with a clear, accurate and well governed data model at the core of our systems. This allows information-based decision making, the ability to utilise real time technologies and make the best use of emergent technology such as robotics and predictive analytics.
- **Deliver technology that drives business innovation and operational efficiencies** – We aim to deliver technology solutions that support the wider business strategy focused on Customer, Efficiency and Safety.
- **Simplification of systems and applications** – We aim to operate a simple applications and infrastructure landscape, that meets the needs of the organisation whilst ensuring a cost effect and well understood and manageable IT operation.

The strategic objectives that drive our approach to cyber security are:

- **Proactive Risk Management** – We aim to enable data owners and administrators to be more aware of the security risks that their information and technology assets are vulnerable to, identify controls to reduce those risks, and understand what risks remain after any identified controls have been implemented. Initiatives that support this objective will support a defence in depth architecture and provide increased security and resilience of our critical services. Some of these initiatives and supporting projects are required to be in place according to UK and EU legislation.
- **Data as an Asset** – We aim to treat data as asset, that is properly classified, handled, protected and disposed of in an appropriate manner befitting of the asset. This will ultimately help us reduce the likelihood of data loss and disclosure of classified & protected data.
- **Proactive Security Operations** – We aim to be able to recover information and technology assets in the event of an incident or crisis. Additionally, to proactively manage the security of the estate using prevention, detection and vulnerability assessment tools whilst evolving membership of forums and wider industry groups on cyber security.
- **Security Aware and Security Conscious Employees** – We aim to ensure all colleagues and suppliers understand the risks involved with information and data, undergo regular training and awareness sessions around increasing cyber threats and foster a culture that the responsibility of security is everyone's and that proactive identification is to the benefit of everyone.
- **Improved Governance and Compliance** – We aim to have robust governance and compliance controls are in place to support and guide colleagues to work safely, securely and within UK and Industry regulations.
- **Improved Physical and Environmental Controls** – We aim to secure all technology assets and people so that safe and secure working environments are always ensured and maintained.

How will we understand if the spend has been successful?

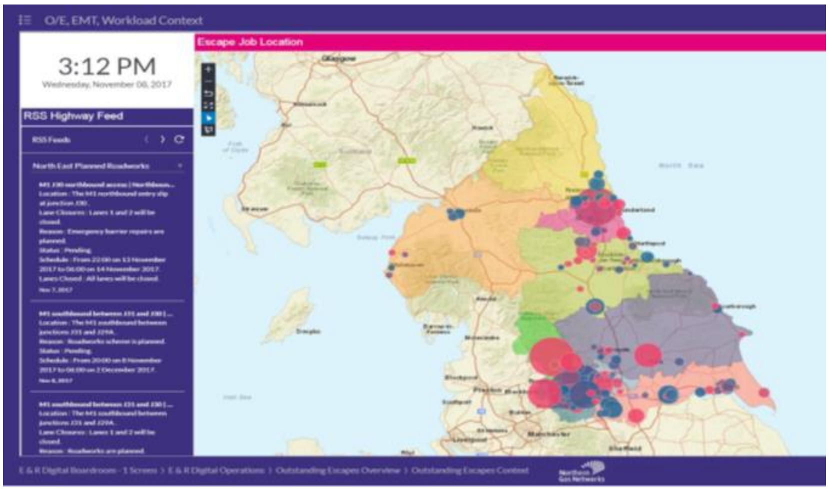
If we can achieve the following four key objectives, then investment in Technology & Systems during RIIO-2 will have been a success:

- **Deliver value** – Delivering measurable benefits, creating sustainable long-term valve
- **Improved customer experience** – seamless experience, informative communications, reduced query resolution times

- **Make data open and accessible** – Provide technology that gives full access to use data, build information and collaborate with others
- **Colleagues needs first** – Working with our colleagues to understand and best support business needs
- **Secure** – Building resilience into everyday operations, enabling a safe and secure environment to nurture innovation
- **Keep it simple and standard** – Creating services which can evolve quickly in line with changing internal and external demands

4.1. Narrative Real-Life Example of Problem

The Digital Operations Room – We collect and store a huge amount of data. This drives the decisions that we make every day. Visualising that data, transforming it into useful information, is a continuous challenge, and we identified a need for a single, consistent platform to control, present and publish the management information that is vital to the operation of a safe, efficient and customer-focussed network.


O/E, EMT, Workload Context
3:12 PM
Wednesday, November 08, 2017
RSS Highway Feed
RSS Feeds
North East Planned Roadworks
Escape Job Location
Glasgow
Sunderland
Hartlepool
Scarborough
North Sea
Barrow-in-Furness
Blackpool
Preston
Southport
Manchester
Liverpool
Sheffield
E & R Digital Boardroom - 1 Screen › E & R Digital Operations › Outstanding Escapes Overview › Outstanding Escapes Context
Northern Gas Networks

M1 J30 northbound access | Northbound...
Location : The M1 northbound entry slip at junction J30.
Lane Closures : Lanes 1 and 2 will be closed.
Reason : Emergency barrier repairs are planned.
Status : Pending.
Schedule : From 22:00 on 13 November 2017 to 06:00 on 14 November 2017.
Lanes Closed : All lanes will be closed.
Nov 7, 2017

M1 southbound between J31 and J30 | ...
Location : The M1 southbound between junctions J31 and J29A.
Reason : Roadworks scheme is planned.
Status : Pending.
Schedule : From 20:00 on 8 November 2017 to 06:00 on 2 December 2017.
Nov 6, 2017

M1 southbound between J31 and J30 | ...
Location : The M1 southbound between junctions J31 and J29A.
Lane Closures : Lanes 1 and 2 will be closed.
Reason : Roadworks are planned.

We developed the Digital Operations Room, a browser-based platform that has the capability to integrate multiple data sources and visualise information in fully interactive, multi-layered dashboards.

The image above shows the use of the Digital Operations Room to visualise the near real-time status of gas escapes. This is further augmented with information from the UK Highways Agency to bring real-time traffic disruption information. This will enable us to define business prioritisation quicker when multiple gas escapes or incidents occur, helping us to prioritise engineering works to pro-actively avoid gas leaks occurring and improve network resilience.

SCADA on AWS - SCADA is the control system utilised by us to monitor and manage the flow of gas throughout the network. SCADA has traditionally been hosted on servers maintained and supported within NGNs infrastructure. SCADA system into AWS and Routing telemetry traffic into AWS project had the commercial aim to reduce the computer infrastructure costs for us and to improve the ability of the gas-distribution-network systems to scale in the future. To achieve this commercial aim, appreciable improvements in application virtualisation to enable SCADA and Telemetry to run on a cloud computing environment.

At the time, there were no readily available sources of knowledge that detailed how these designs could be achieved. We were one of the first companies in the world to develop the knowledge required to achieve a cloud transfer for complex SCADA and Telemetry systems that supervised, monitored and controlled a national-scale sensory infrastructure. Other world leading experts (e.g. Schneider SCADA) who had detailed knowledge of SCADA, Telemetry and Cloud technology had considered virtualisation of SCADA and Telemetry to be practically non-viable and had no suggested methods how to do it. We developed application virtualisation designs that appreciably improved the baseline in cloud-virtualisation capabilities, meaning that running SCADA on a cloud computing environment became a viable option.

SCADA on AWS is now fully operational, managing over 37 million meters of pipes, with hundreds of thousands of sensors. NGNs design and experience are now attracting a great deal of interest from other companies worldwide.

4.2. Spend Boundaries

The boundaries of spend proposed by this justification paper include capital investment on the assets listed in Section 3. It does not include any operational costs associated with running this equipment.

5. Probability of Failure

The probability of Failure (PoF) is the probability an asset will fail at a given point time. When justifying our RIIO-2 capital investment, our Cost Benefit Analysis uses expertly elicited failures rates due to there being no industry standard failure rates for information technology assets (both tangible and non-tangible).

Types of Failure

- Avoided Colleague Care costs
- Avoided productive time lost
- Avoided GDPR fine
- Avoided NIS fine
- Avoided impact of H&S incidents
- Avoided opex and training costs
- Productivity improvements
- Avoided implementation of our Telemetry Black Plan
- Avoided impact on billing equipment and costs
- Avoided loss of supply incidents

Rate of Failure

The following PoF rate assumptions have been used in our Cost Benefit Analysis.

Device and hardware

The failures associated with IT hardware can be categorised as productivity and chance of fine risk. The below detail the assumptions we have used.

Productivity:

- Per annum increase, after 2 years for 2 years, of IT support costs and productivity costs from ceasing hardware upgrades – **25%**
- Per annum increase, thereafter, of IT support costs and productivity costs from ceasing hardware – **2.5%**

Fine:

- Baseline probability of fine related to hardware vulnerability in FY 2021/22 – **2%**
- Rate at which this risk increases if proactive replacement is stopped – **2.5%**
- Probability of NIS fine due to hardware vulnerability – **2%**
- Probability of GDPR fine due to hardware vulnerability – **25%**

Software

The failures associated with IT hardware can be categorised as productivity and chance of fine risk. The below detail the assumptions we have used.

Productivity:

- Per annum increase of IT support costs and productivity costs from ceasing software upgrades – **10%**
- Per annum increase of telemetry blackout costs from ceasing software upgrades – **10%**

Fine:

- Baseline probability of fine related to hardware vulnerability in FY 2021/22 – **2%**
- Rate at which this risk increases if proactive replacement is stopped – **2.5%**
- Probability of NIS fine due to software vulnerability – **2%**
- Probability of GDPR fine due to software vulnerability – **25%**

Innovation

We see investments in Innovation resulting in safer working, better decision making, improved risk assessment and repair/replace decisions. For this reason, the CBA has included impacts on customer time impacts, gas in buildings and probability of fatality and non-fatality injuries. All health and safety and gas in building assumptions used in the CBA are from the NARMs methodology. The below document the assumptions:

- Probability of an explosion given a GIB (PoF) – **0.076%**
- Probability of an explosion causing a death (PoC) – **45%**
- Probability of explosion causing a minor injury (PoC) – **100%**
- Probability of explosion causing building damage (PoC) – **100%**

Cyber Security

The failures associated with cyber security can be categorised as productivity and chance of fine risk. The below detail the assumptions we have used.

Productivity:

- Per annum increase, after 2 years for 2 years, of IT support costs and productivity costs from ceasing hardware upgrades – **25%**
- Per annum increase, thereafter, of IT support costs and productivity costs from ceasing hardware – **2.5%**

Fine:

- Baseline probability of fine related to hardware vulnerability in FY 2021/22 – **2%**
- Rate at which this risk increases if proactive replacement is stopped – **2.5%**

- Probability of NIS fine due to hardware vulnerability – **2%**
- Probability of GDPR fine due to hardware vulnerability – **25%**

5.1. Probability of Failure Data Assurance

Our probability of failure data has been expertly elicited as there are no industry standard failure rates for information technology assets. We have been conservative on the probabilities used to ensure that any investments we are planning will provide the level of benefits we are estimating.

6. Consequence of Failure

As can be seen above, the consequence of failure, generally falls into two main categories, loss of productivity and risk of fine.

Loss of productivity can have a severe impact on business performance, it can be wide ranging from something as simple as colleagues in the back office being unable to perform their duties, such as designing projects, to IT systems failing linked to attending gas escapes. We have made the following assumptions in our Cost Benefit Analysis:

- Cost per hour of IT Support - **£26**
- Cost per hour of NGN employee time - **£24**
- Assumed average support time per failure – **2 hours**
- Assumed average productive time lost per hardware failure – **16 hours**
- Assumed average cost per device replacement, excluding monitors - **£568**
- Assumed average productive time lost per software outage – **4 hours**
- Assumed average NGN employee time per unplanned interruption – **3 hours**
- Assumed average NGN customer time per unplanned interruption – **3 hours**
- Assumed average NGN employee time per planned interruption – **2 hours**
- Assumed average NGN customer time per planned interruption – **2 hours**
- Assumed average support time per non-email spam incident – **3 hours**
- Assumed average productive time lost per non-email spam cyber security incident – **4 hours**
- Assumed average support time per email spam incident – **0.5 hours**
- Assumed average productive time lost per email-spam cyber security incident – **0.5 hours**

The risk of being fined by the new GDPR and NIS legislation is increasing as we face a world where cyber attacks are more prevalent and the impacts of which could affect asset performance or sensitive data. We have made the following assumptions in our Cost Benefit Analysis:

- NIS Fine per incident where 5000 customers or more are off gas - **£17m**
- GDPR fine applicable to NGN - **£40m**

7. Options Considered

We have undertaken our Cost Benefit Analysis at strategy level where the benefits from intervention are common and can be grouped to provide the net present value of an investment decision. For clarity CBA's have been undertaken at the following levels:

- Devices and hardware

- Software
- Innovation
- Cyber Security

We have not included a Cost Benefit Analysis within this paper for our Network strategy, as the proposed investment is below Ofgem's materiality threshold.

The investment options considered for this asset class are listed below and have the following in common:

- All options use standard unit costs for different types of assets and interventions which have been derived from historical costs. For more information on unit costs see Section 7.3.
- The programme of works will be delivered evenly over the five-year price control period.
- The primary benefit delivered by these intervention options is a reduction compliance risk (i.e. fines) and improvement in productivity compared to baseline.

7.1.1. Baseline – Do nothing / minimum

This option is used as the baseline for which all other options are measured against. It does not include any capital investment but instead considers the cost of ongoing maintenance activities and repairs on failure. There are no direct benefits accrued under this option however it does include societal impacts associated with leakage, fatality and injury.

7.1.2. Option 1 – RIIO-2 Preferred Strategy

This option sets to achieve our objectives for RIIO-2. We have modelled the impact (both cost and service) through Ofgem's CBA model using standard assumptions which are listed in sections 5 and 6.

7.1.3. Option 2 – Deferred investment

This option considers the effects of deferring all capital investment until RIIO-3.

7.1.4. Option 3 – Reduced Expenditure

This option has modelled impact of a reduced capital expenditure on cost and service to see whether this option adds more value at a lesser cost than our preferred strategy.

7.1.5. Option 4 – Increased Expenditure

This option has modelled impact of an increased capital expenditure on cost and service to see whether this option adds more value at a higher cost than our preferred strategy.

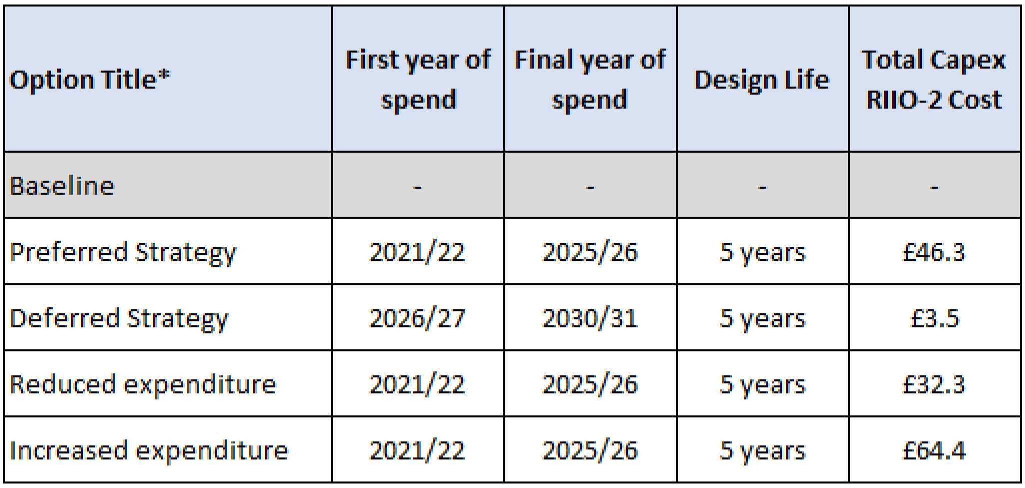
Future Energy Pathways

We have gone with the default assumption of current assumed proportion of methane CO2 in natural gas projected forwards due to uncertainties in the potential energy pathways and because this is reflective of the current gas quality legislation. However, we acknowledge that significant changes to gas demand or the allowed methane content of gas, for example due to the blending with or conversion to hydrogen, would impact the benefits of our investments.

Arup conducted analysis on the potential benefits of our H21 Programme (see A13 - NGN RIIO-2 Consumer Value Proposition) that showed 45% of the gas in our network is expected to be Natural, 15% biomethane and the remaining 40% hydrogen by 2040; due to a combination of blending and sub-areas of our networks being fully converted. This is consistent with Net-zero by 2050 aligned with the ENA Navigant report.

We have not explicitly modelled changes in the methane content of gas in our CBAs, as overall gas demand and the change in C02 content of the gas is not expected to be different enough to materially impact the NPV, Payback & Option Ranking of our preferred investment programme. This is because carbon risk benefit is only one element of overall risk benefit and this will be reduced by up to 40% by 2040 across all scenarios if the ambitious but realistic ENA Navigant report pathway is chosen. Our chosen programme represents value for money over a 20-year period regardless and is mainly driven by financial benefits such as avoiding colleague care costs. The investments also ensure that we are compliant with relevant legislation. Our strategy therefore represents a no regrets investment programme that is consistent with net zero and will deliver value to customers whether a hydrogen or electrification pathway is chosen.

7.2. Options Technical Summary Table

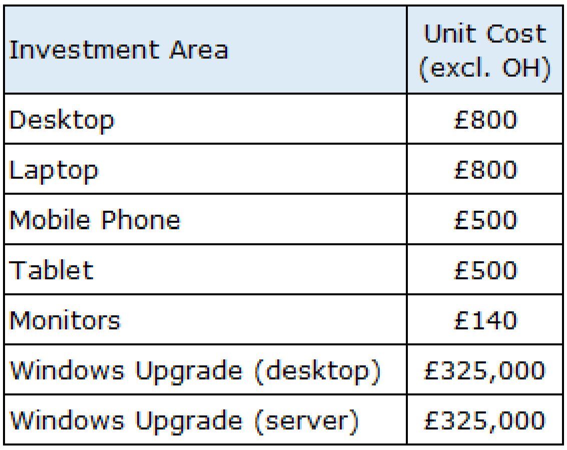


Option Title*	First year of spend	Final year of spend	Design Life	Total Capex RIIO-2 Cost
Baseline	-	-	-	-
Preferred Strategy	2021/22	2025/26	5 years	£46.3
Deferred Strategy	2026/27	2030/31	5 years	£3.5
Reduced expenditure	2021/22	2025/26	5 years	£32.3
Increased expenditure	2021/22	2025/26	5 years	£64.4

*Note these costs exclude our Network Strategy which is below Ofgem's materiality threshold for a CBA.

7.3. Options Cost Summary Table

Where there are unit costs involved in this work, these are detailed in the table below and include our overheads in managing the roll out of these projects. However, due to the nature of IT projects, unit costs can't always be applied, and rather project estimates need to be calculated based on similar historic projects. For example, where we are planning a GIS mapping software upgrade, we have used our historic costs to forecast the cost of this project.



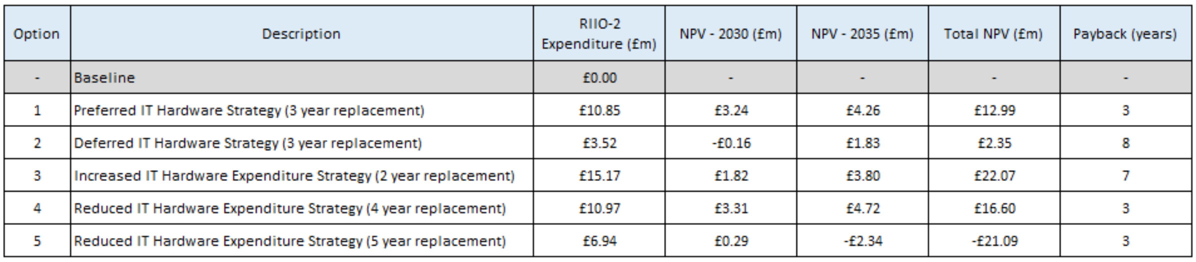
Investment Area	Unit Cost (excl. OH)
Desktop	£800
Laptop	£800
Mobile Phone	£500
Tablet	£500
Monitors	£140
Windows Upgrade (desktop)	£325,000
Windows Upgrade (server)	£325,000

8. Business Case Outline and Discussion

8.1. Key Business Case Drivers Description

The tables below show the results of each option compared to the baseline and the following narrative then discusses the strengths and weaknesses of each.

Devices and hardware



Option	Description	RIIO-2 Expenditure (£m)	NPV - 2030 (£m)	NPV - 2035 (£m)	Total NPV (£m)	Payback (years)
-	Baseline	£0.00	-	-	-	-
1	Preferred IT Hardware Strategy (3 year replacement)	£10.85	£3.24	£4.26	£12.99	3
2	Deferred IT Hardware Strategy (3 year replacement)	£3.52	-£0.16	£1.83	£2.35	8
3	Increased IT Hardware Expenditure Strategy (2 year replacement)	£15.17	£1.82	£3.80	£22.07	7
4	Reduced IT Hardware Expenditure Strategy (4 year replacement)	£10.97	£3.31	£4.72	£16.60	3
5	Reduced IT Hardware Expenditure Strategy (5 year replacement)	£6.94	£0.29	-£2.34	-£21.09	3

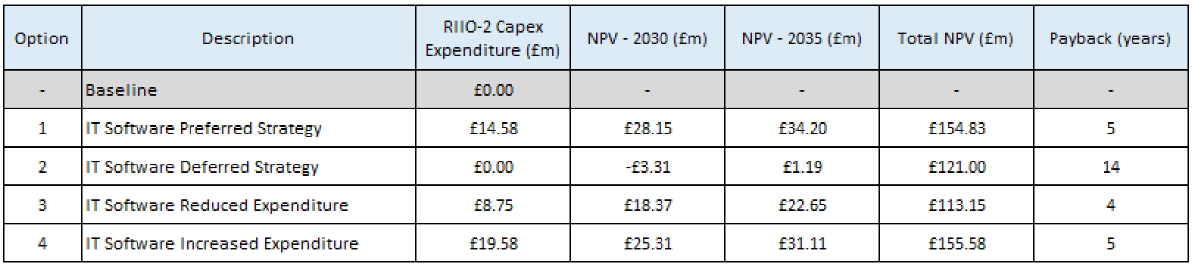
The benefits of investing in Hardware projects relate to a reduction in cyber security fines and an improvement in productivity compared to the baseline. There is a short payback to completing this work and is in line with replacement cycles meaning the investment will pay back over the life of the assets.

Any capital investment in RIIO-2 delivers a significant benefit compared to deferral to RIIO-3 as can be seen by the NPV in every year. Increasing expenditure by replacing hardware every 2 years instead of 3 years leads to a higher total Net Present Value however this is only after 16 years which is beyond the expected asset life of the equipment. Reducing expenditure by replacing hardware every 4 or 5 years instead of 3 years leads to the same NPV after 3 years however the 4 year cycle, Option 4, has the best NPV at 4 years and the 5 year cycle, Option 5, has the best NPV at 5 years, after which the 3 year cycle, Option 1, is best. The difference in benefit between Option 1 and Option 4 and 5 is that there is a decrease in productivity in RIIO-2 under Option 4 and 5 as our staff will be operating older machines, however Option 1 shows a decrease in productivity in RIIO-3 as we are only modelling capital replacements in RIIO-2. Whereas we would expect this capital programme to continue in RIIO-3 and so in reality we wouldn't see this drop in productivity and Option 1 would continue to have the highest NPV in every year. Our preference is not to have a decrease in productivity in RIIO-2, therefore replacing Hardware every 3 year is our preferred option.

Deferring investment clearly has the lowest capital expenditure in RIIO-2 being zero however after 8 years this is not the case and considering maintenance and repair costs this option is only the cheapest option for the first five years. Options 1, 4 and 5 have the lowest capex costs for the first 3 years, Option has in year 4 and Option 5 has in year 5, after which Option 1 is lowest until 2028. The same can be said for Totex however Option 3 is lowest for one year longer until 2029.

We have completed sensitivity on the preferred option. As noted above, the main benefit is in relation to productivity. To complete the sensitivity analysis, we have halved the productivity improvement between Baseline and Option 1 to assess the impact. This increases the payback to 6 years and demonstrates this option provides benefit under this sensitivity and therefore even at this lower tolerance is a worthwhile investment.

Software



Option	Description	RIIO-2 Capex Expenditure (£m)	NPV - 2030 (£m)	NPV - 2035 (£m)	Total NPV (£m)	Payback (years)
-	Baseline	£0.00	-	-	-	-
1	IT Software Preferred Strategy	£14.58	£28.15	£34.20	£154.83	5
2	IT Software Deferred Strategy	£0.00	-£3.31	£1.19	£121.00	14
3	IT Software Reduced Expenditure	£8.75	£18.37	£22.65	£113.15	4
4	IT Software Increased Expenditure	£19.58	£25.31	£31.11	£155.58	5

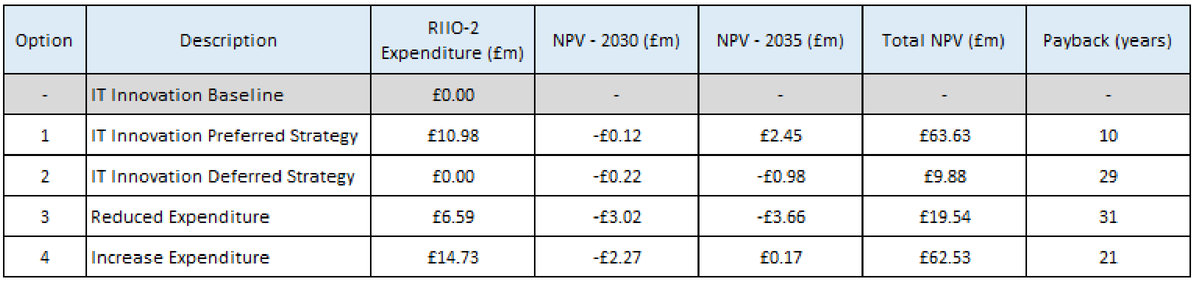
The benefits of investing in Software projects relate to a reduction in software vulnerability fines and an improvement in productivity compared to the baseline. There is a short payback to completing this work and is in line with software upgrade cycles meaning the investment will pay back over the life of the upgrade. The investment delivers a significant benefit compared to deferral to RIIO-3 as can be seen by the total NPV.

We have also modelled the impact of reducing expenditure, and therefore delivering fewer projects, and increased expenditure, delivered additional projects.

The net present value results show that there is lower value delivered through both these options. For reduced expenditure, the projects that have been removed still provide value over and above the capital expenditure required. Although this has a payback that is shorter than the preferred strategy, the NPV demonstrates it offers significantly lower value. Where we have increased expenditure, the CBA demonstrates that these additional projects offer incrementally little benefit over the capital expenditure required.

Like Hardware, the main benefit of investing this option is productivity. We have taken a similar approach to Hardware and halved the benefit associated with this to assess the sensitivity. It shows there is a payback of 6 years and therefore even at this lower tolerance is a worthwhile investment.

Innovation



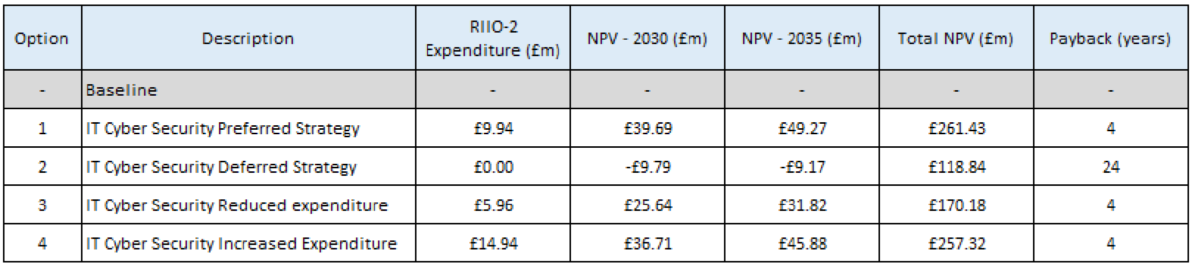
Option	Description	RIIO-2 Expenditure (£m)	NPV - 2030 (£m)	NPV - 2035 (£m)	Total NPV (£m)	Payback (years)
-	IT Innovation Baseline	£0.00	-	-	-	-
1	IT Innovation Preferred Strategy	£10.98	-£0.12	£2.45	£63.63	10
2	IT Innovation Deferred Strategy	£0.00	-£0.22	-£0.98	£9.88	29
3	Reduced Expenditure	£6.59	-£3.02	-£3.66	£19.54	31
4	Increase Expenditure	£14.73	-£2.27	£0.17	£62.53	21

There is no material factor that demonstrate benefits of investing in Innovation Projects. Instead, the benefits come from a range of impacts including a reduction in customer waiting time and safety impacts. The payback for investments in innovation are longer than the previous investment areas however the benefits from innovation are far reaching and delivered for longer periods. The investment delivers a significant benefit compared to deferral to RIIO-3 as can be seen by the total NPV.

We have again modelled the impact of reducing the number of projects completed and increasing the number of projects completed. In both cases the CBA results demonstrate that these options offer lower value and therefore have a longer payback period. Therefore, these options are not the preferred options.

As noted above, there is no single material factor that contributes to the value from Innovation investments. To model the sensitivity, we have looked at the benefits achieved in RIIO-2. Net of the capital expenditure there are c.£16m of benefits from the preferred option compared to baseline. We have halved this benefit and it changes the payback to 20 years which we consider is a reasonable range on the payback and therefore even at this lower tolerance is a worthwhile investment.

Cyber Security



Option	Description	RIIO-2 Expenditure (£m)	NPV - 2030 (£m)	NPV - 2035 (£m)	Total NPV (£m)	Payback (years)
-	Baseline	-	-	-	-	-
1	IT Cyber Security Preferred Strategy	£9.94	£39.69	£49.27	£261.43	4
2	IT Cyber Security Deferred Strategy	£0.00	-£9.79	-£9.17	£118.84	24
3	IT Cyber Security Reduced expenditure	£5.96	£25.64	£31.82	£170.18	4
4	IT Cyber Security Increased Expenditure	£14.94	£36.71	£45.88	£257.32	4

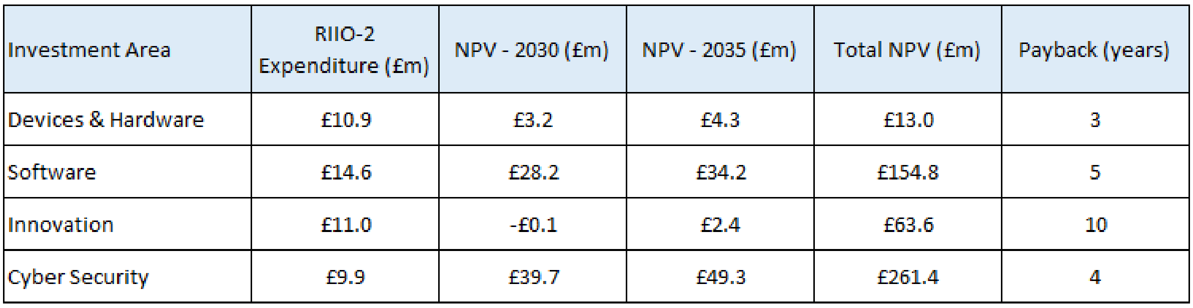
The benefits of investing in Cyber Security related projects means we significantly reduce the chance of a breach and subsequent fine. Due to the high cost of consequence, there is a short payback to completing this work where and the investment delivers a significant benefit compared to deferral to RIIO-3 as can be seen by the total NPV.

The alternative options investigated show similar results to the other areas of expenditure. When we have modelled either increasing or reducing our expenditure, the CBA results demonstrate that these options offer lower value than our preferred strategy.

To complete the sensitivity in this area, both the risk of a Cyber Security fine and productivity have significant impact. So, the benefit of both factors has been halved in a sensitivity scenario. This shows that the payback increases to 5 years and therefore even at this lower tolerance is a worthwhile investment.

8.2. Business Case Summary

The table below summarises the results of the preferred option CBAs.



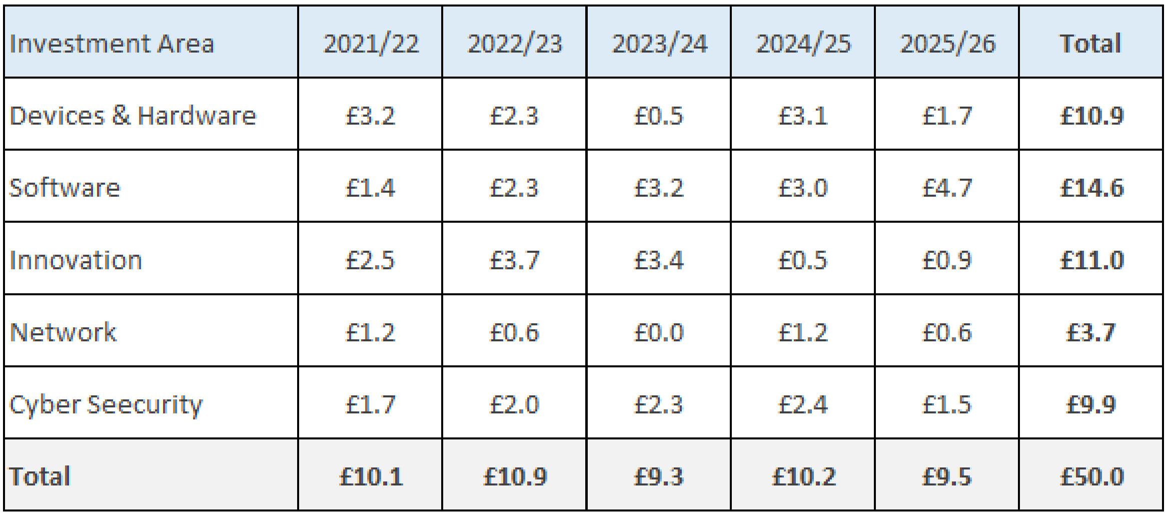
Investment Area	RIIO-2 Expenditure (£m)	NPV - 2030 (£m)	NPV - 2035 (£m)	Total NPV (£m)	Payback (years)
Devices & Hardware	£10.9	£3.2	£4.3	£13.0	3
Software	£14.6	£28.2	£34.2	£154.8	5
Innovation	£11.0	-£0.1	£2.4	£63.6	10
Cyber Security	£9.9	£39.7	£49.3	£261.4	4

9. Preferred Option Scope and Project Plan

9.1. Preferred Option

Our preferred options are shown above. The table in Section 9.2 shows a more detailed breakdown of the investments.

9.2. Asset Health Spend Profile



Investment Area	2021/22	2022/23	2023/24	2024/25	2025/26	Total
Devices & Hardware	£3.2	£2.3	£0.5	£3.1	£1.7	**£10.9**
Software	£1.4	£2.3	£3.2	£3.0	£4.7	**£14.6**
Innovation	£2.5	£3.7	£3.4	£0.5	£0.9	**£11.0**
Network	£1.2	£0.6	£0.0	£1.2	£0.6	**£3.7**
Cyber Seecurity	£1.7	£2.0	£2.3	£2.4	£1.5	**£9.9**
Total	**£10.1**	**£10.9**	**£9.3**	**£10.2**	**£9.5**	**£50.0**

The total forecast capital expenditure for Technology & Systems has been included within this Cost Benefit Analysis and can be referenced back to the following documents:

- RIIO-2 Business Plan – Tables 6.9
- RIIO-2 Business Plan Data Tables – Table 3.05
- A23.J - NGN RIIO-2 Investment Decision Pack – Technology & Systems (Hardware) – CBA
- A23.J - NGN RIIO-2 Investment Decision Pack – Technology & Systems (Software) - CBA
- A23.J - NGN RIIO-2 Investment Decision Pack – Technology & Systems (Innovation) - CBA
- A23.J - NGN RIIO-2 Investment Decision Pack – Technology & Systems (Cyber Security) - CBA

9.3. Investment Risk Discussion

Technology and Systems is a relatively large asset population and wide ranging. In addition, technology changes quickly that there is uncertainty around some areas of the unit costs. We expect to be managing this risk and optimising our spend in this area accordingly. Therefore, we expect to manage these risks within our overall capital spend.