

Engineering Justification Paper

# Back office system replacement

Version: Final

Date: December 2019

Classification: Highly Confidential

Reference: SGN IT – 002 BO EJPDec19



# 1 Table of Contents

<b>1 Table of Contents</b> .....	<b>2</b>
<b>2 Introduction</b> .....	<b>4</b>
2.1 General Background .....	4
2.2 Site Specific Background.....	5
<b>3 Equipment Summary</b> .....	<b>6</b>
<b>4 Problem Statement</b> .....	<b>6</b>
4.1 Narrative Real-Life Example of Problem .....	7
4.2 Spend Boundaries.....	7
<b>5 Probability of Failure</b> .....	<b>7</b>
5.1 Probability of Failure Data Assurance .....	8
<b>6 Consequence of Failure</b> .....	<b>8</b>
<b>7 Options Considered</b> .....	<b>9</b>
7.1 Oracle’s EBusiness Cloud .....	10
7.2 SAP Cloud ERP.....	10
7.3 Options Technical Summary Table .....	11
Oracle EBS Cloud migration summary:.....	11
SAP Cloud ERP migration summary:.....	11
7.4 Options Cost Summary Table .....	12
Oracle EBS Cloud cost summary:.....	12
SAP Cloud ERP cost summary:.....	13
<b>8 Business Case Outline and Discussion</b> .....	<b>14</b>
8.1 Key Business Case Drivers Description .....	14
8.2 Business Case Summary .....	16
<b>9 Preferred Option Scope and Project Plan</b> .....	<b>17</b>
9.1 Preferred option .....	17
9.2 Asset Health Spend Profile .....	17
9.3 Investment Risk Discussion .....	18
<b>Appendix A - Acronyms</b> .....	<b>21</b>

## Figures:

Figure 1: Back office integrations and ecosystem at SGN. ....	5
Figure 2: Back office technical scope.....	8

**Tables:**

Table 1:	Consequence of failure to invest in back office replacement. ....	9
Table 2:	Cost breakdown for the preferred option. ....	12
Table 3:	Cost breakdown by activity type for the preferred option.....	12
Table 4:	Cost breakdown for the second option. ....	13
Table 5:	Cost breakdown by activity type for the second option.....	13
Table 6:	Key value drivers in options analysis. ....	15
Table 7:	Summary of CBA results.....	15
Table 8:	Business case matrix. ....	16
Table 9:	Asset health spend profile. ....	17
Table 10:	Risk Matrix .....	18
Table 11:	Sensitivity risk analysis.....	19
Table 12:	Capitalisation rate sensitivity .....	20

## 2 Introduction

Back Office systems enable SGN to run Finance, HR and Procurement services which are essential to our operation. Back Office systems enable the payment of employees, contractors and suppliers and support the full end to end procurement process for purchasing essential services, tools, equipment and materials required to ensure SGN can safely manage and maintain our network. The Back-Office applications enable essential reporting of financial and employee data including but not limited to end of year statutory accounts and our RRP returns. Throughout GD1 there has been a requirement to update and change SGN Back Office applications in response to legislative and mandatory change critical to our HR, Finance and Procurement services.

Also, in order to continue to have our systems maintained and supported by our support vendors we have received and must continue to receive, supporting application features that are needed to upgrade and refresh the existing applications and estate. Without these, SGN would risk security weaknesses, degraded performance of the platforms and non-compliance with statutory changes such as HMRC tax changes. Our Oracle roadmap and wider Finance, HR and Procurement systems will require a “like for like” upgrade and refresh where end of life services exist, these will require replacement during GD2.

This paper provides an engineering justification to SGN’s proposal on undertake the minimum mandatory work required to keep our existing systems and estate in supported and functioning during the GD2 timeframes. It should be noted that the operating costs within SGN’s business plan, including the built-in efficiency, cannot be achieved without the required investment in upgrading and replacing ageing and end of life systems.

### 2.1 General Background

Our current back office systems were first implemented in 2009 and have undergone significant changes from time to time, through supplier provided patches, upgrades, infrastructure refreshes and changes to reflect the structural needs of our business as it has changed throughout GD1. SGN’s current main platform, **Security** application is currently cited as reaching end of life (EOL) from September 2023 with no release dates announced for future versions after **Security** do not currently offer any clear path forward other than to migrate to the **Security** (offered as SaaS - Software as a Service) solution. SGN will also take this opportunity to migrate bespoke **Security** forms applications for contractor invoicing and payments system into **Security**

At this time, if alternative pathways exist to achieve the same outcome they will be considered but at the time of writing this paper, none exist.

The **Security** platform serviced by the globally recognised IT vender **Security** may offer for a limited time an extended supported contract from September 2023 until SGN can upgrade or replace the system. However, it is inevitable that SGN will be required to pay significantly more in extended support costs to the supplier for this arrangement. The extended support contract only provides critical and security related patching from the supplier which means any new regulatory or other significant changes cannot be incorporated into the product and would need manual & high cost workarounds by SGN. Therefore, this option has been discounted as it is not cost effective.

# Security

Figure 1: Back office integrations and ecosystem at SGN.

Our Customer Engagement Group (CEG) and wider customer advice, told us that they expect us to seek advice from technical and industry experts to validate the areas of technology that we should be investing in and the associated levels of spend. Upon reviewing our plan with the CEG there was a stated expectation that SGN get independent validation of their IT investment plans to ensure proposed investment is in the correct areas and the value we are expecting to spend is in line with industry analyst predictions. The IT business plan has been validated by Gartner (see supporting information Gartner benchmark report) and the proposed spend on replacing back office systems is moderately placed when compared to their benchmark range. This is also SGN's experience from various independent industry forums, publications and our key technology suppliers, as evidenced in this paper and our historical expenditure on this platform.

Reduced or no direct investment in an ageing system from time to time results in increased risks of failures and higher operational costs to cater for compensating workarounds and controls and / or maintaining an obsolete or unsupported technology estate. No investment in replacing an unsupported back office will also create operational risks for SGN due to high failure rates and lack of supplier support available on the technology platforms that are essential to run the business. Ultimately, not investing in these areas could directly impact customers with critical services such as gas escape response or our mains replacement programme being impacted if our suppliers or staff aren't paid on a timely and accurate manner.

## 2.2 Site Specific Background

The technology referenced in this document will underpin our corporate functions serviced out of our head office in Horley, our other satellite offices and depots across the country. The deployment

of the new technology solution referenced in this paper is likely to be within **Security** with no physical deployment at or in any SGN location.

### 3 Equipment Summary

#### Back office systems replacement

SGN plans to migrate our **Security**. In doing so, we plan to decommission our contractor payment and invoice processing be-spoke applications into standard **Security** features.

After initial evaluation, **Security** is our preferred option. The deployment of **Security** Cloud will provide SGN the most integrated solution for our core back office functions with minimum disruption to our operations and low impact on our current process and staff readiness.

We have estimated the cost to move to **Security** to be £4M, spread over 3 years. The cost includes SaaS licenses, project management, data transfer, integration and training.

Technical skills development and internal capability building within SGN will also be an element of this investment.

### 4 Problem Statement

Global technology shifts are fast paced and difficult to predict accurately. To prove this point, at the beginning of GD1, none of our workforce had or made use of smart phone technology and were utilising one mobile application for basic data gathering on laptops. Equally, customers' expectations around digital interactions were limited to a simple, basic website. Now, at the end of the same price control the mobile revolution has transformed the daily life of all humans and digital disruption has transformed multiple industries.

SGN is proposing to replace its current back office systems which, during GD2 will become unsupported platform at the beginning of the GD2 timelines. Currently operational, the **Security** will be out of support from Sep 2023. After this time the product would be on extended support with additional cost for the same or reduced features thereafter. During the extended support, the product will only be serviced for critical security updates that means there will be no feature enhancement or fixes supplied by the vendor.

Continuing with **Security** beyond September 2023 will provide a significant risk to SGN. Our back-office systems are essential to ensuring our employees and contractors are paid and that we can procure materials, services, tools and equipment to run operations safely on a daily basis. SGN will be required to apply support patches and upgrades to ensure compliance with legislation including GDPR, Employment Law, Health and Safety as well as annual updates received from HMRC. Many of these patches are available from the supplier under the normal support contract but will not be in an extended support contract arrangement.

SGN must highly accurate and transparent through an externally audited process across our payroll, procurement and accounting processes. Our back-office systems are critical in the production of our end of year reporting enabling us to adhere to financial accounts and company reporting rules. The risk of failure on these applications becomes critical to our ability to operate as we will be unable to procure materials and equipment, pay our employees and contractors and run our financial processes. Ultimately, not investing in these areas could directly impact customers with critical

services such as gas escape response or our mains replacement programme being impacted if our suppliers or staff aren't paid on a timely and accurate manner.

Upon engagement with the CEG we were advised to seek advice from technical and industry experts to validate the level of spend and that we were spending in the right areas. Upon reviewing our plan with the CEG group it was clear there was also an expectation that SGN get independent validation of their IT investment plans to ensure proposed investment is in the correct areas and the value we are expecting to spend is in line with industry analyst predictions. The IT business plan has been validated by Gartner (report available as part of GD2 submission) and the proposed spend on back office replacement is defined by them as moderately placed when compared to their benchmark range.

#### 4.1 Narrative Real-Life Example of Problem

During GD1, SGN experienced technical issues on our Back-Office systems that resulted in a brief period when payments to suppliers were taking longer than expected to process by us due to system problems. These delays in processing payments, in turn, resulted in numerous issues with our third-party suppliers, in particular, those supporting our mains replacement programme who are often, small, independent and cash sensitive companies who cannot withstand several weeks delay in receiving payments as it can result in them running out of cash. During this time, several of the suppliers had to threaten the withdraw of services to SGN if the problems were not rectified urgently. Thus, directly affecting our operational business. Several of our suppliers supporting corporate functions such as IT, also had to make the same threat. Fortunately, in this case the issues were ultimately resolved but this example highlights a situation that would not have been tenable and would have resulted in our business not being able to fulfil its day to day operational duties. Ultimately, further work on improving our Back-Office systems resolved the matter and service was returned to normal.

#### 4.2 Spend Boundaries

A migration of SGN deployment of **Commercial Confidentiality**, **Commercial Confidentiality** and **Commercial Confidentiality** will be in scope. The deployment will make use of the Cloud technology, running the systems on a pay by subscription basis (SaaS service).

We have estimated the overall cost to migrate over three years will be £4M. The cost includes SaaS licenses, project management, data transfer, integration and training.

Technical skills development and internal capability building within SGN will also be an element of this investment. Along with the project costs, that will largely be capitalised, there will an ongoing opex cost required to run, enhance, maintain and replace the services from time to time that will be in line with the current system maintenance costs built in our IT opex costs to run our systems.

## 5 Probability of Failure

The investment case presented is for information technology therefore cannot be linked directly to engineering equipment failures. However, failures in financial accounting, invoice processing, contractor payment and HR systems will result in significant risks for SGN operations and increased

cost for service. We know that the current end of life for support of our Oracle system is 2023 therefore, failure will be considered inevitable after this point.

The following chart explains the integrated nature of our Back-office systems with the red lined box indicating the current **Security** .

# Security

Figure 2: Back office technical scope

## 5.1 Probability of Failure Data Assurance

The investment case presented is for information technology therefore can be linked directly to engineering equipment.

## 6 Consequence of Failure

The following table outlines the consequence of failing to invest in ongoing support and maintenance of SGN IT assets.

Table 1: Consequence of failure to invest in back office replacement.

Reason for failure	Consequence of Failure
Failure to deliver mandatory change to applications driven by legislative or regulatory requirements	SGN's licence to operate requires us to be compliant with the Uniform Network Code and the Supply Point Administration Agreement. It is critical that we can comply with legislation in regard to how we manage our organisation and run operations on a daily basis. Failure to comply could lead to a breach of licence conditions leading to significant fines or a failure to comply with the law which could lead to fines and / or legal action being taken against SGN.
Failure to carry out upgrade or replacement activity required within 3rd party contracts to remain in support	Critical process and system failures ultimately leading to leading to failure in emergency standards, gas explosion and loss of life (£16m loss of life, up to £100m/10% of turnover fine, unlimited HSE Penalty).
Failure to carry out upgrade or replacement activity due to applications or infrastructure being deemed 'end of life' by 3 <sup>rd</sup> party providers	Loss of licence to operate.
Failure to carry out upgrade or replacement activity driven by the need to remain secure against an ever-increasing cyber security threat	
Failure to carry out upgrade or replacement activity deemed critical by SGN to ensure we continue to meet our licence obligations and regulatory outputs	

Without continued investment in ageing systems, SGN will not be able to keep pace with various industry bodies and its regulatory and statutory obligations. Our ability to delivery our regulatory and statutory repotting will not be possible. Investment in these tools are a 'must' rather than a 'should / could' requirement for Gas Distribution Networks and consequently, are considered mandatory.

SGN's ability to deliver to our financial, employee, supplier and legal obligations would be at a serious risk without a timely investment in refresh, upgrade and where end of life assets exist, replacement of these platforms and systems.

## 7 Options Considered

As there is no clearly define roadmap for the next release of **Security**, there are two broad options available to SGN at this stage. SGN can move the current on premise version **Security** or to invest into a new ERP solution such as from **Security**

SGN's IT strategy is to use Cloud first therefore both options under consideration are based on SaaS offerings with 'always on' infrastructure, high scalability, resilience and security built-in. SaaS offerings are based on a subscription based price model, therefore, no regular investments for patching/upgrading/country customisations required in the future.

As SGN is already a heavy and well established user of **Security** was identified as a clearly the preferred choice based on lowest cost, ease of refresh and migration and adoption. The ability to keep existing interfaces and the familiarity of SGN staff to use **Security** meant this was by far the lowest cost and lowest impact option.

SAP Cloud ERP was also considered, cost estimates were developed based on SGN's previous deployment of a brand-new ERP system in 2009/10. i.e. this would be a completely new process and IT architecture design and major business change.

## 7.1 Oracle's EBusiness Cloud

SGN plans to invest in migration of current on premise **Security** SGN estimates an investment of £4M over three years for the transition to complete.

A project of this nature will be required to run a formal tender process that will be governed by the SGN procurement team working with the project manager. It is quite a common practise for many players to bid for such a transformation project as systems integrators whereas the SaaS licences be procured directly from the service provider – **Security**

The deployment / rollout plans will be synchronised with other activities such as month end /year end closing, financial statement publication, OFGEM reporting etc. in order to minimise interruption to our business and reduce cost. The costs provided are on the basis of SGN historical experience of upgrades and re-platforming of **Security** which is extensive and formally reported on through our RRP process. We have also consulted extensively with the vendor in order to establish the SaaS licence costs, approach to migration and the timeline.

## 7.2 SAP Cloud ERP

The other main, credible option available for SGN is to replace the current on premise **Security** with an alternative ERP system. SAP Cloud ERP was considered as one of the leaders in this area and **Security**. An initial cost estimates was prepared based on SGN's previous deployment of a new ERP system in 2009/10 and through experience shared through our consultation with industry peers and leaders. Expenditure in excess of £22 million were incurred in the process, therefore a conservative £20 million is estimated here for a new ERP implementation. In addition, an overall increase of £2M is estimated as a net increase in regular subscription and support costs due to new technology introduction. It must also be considered that there would be a significant process and change management element to this option (unlike the previous) which would come at a substantial cost.

A project of this nature will be required to run a formal tender process that will be governed by the SGN procurement team working with the project manager. It is quite a common practise for many players to bid for such a transformation project as systems integrators whereas the SaaS licences be procured directly from the service provider – e.g., SAP.

A key assumption made on costs and timeline is on the political certainties, labour and material price stability. It is also assumed that no external or internal significant event/threat occurs that requires a radical re-think of the rollout plans or the use of these technologies.

## 7.3 Options Technical Summary Table

### Security migration summary:

The **Security** is a standard ERP system that has consumed all features from previous on-premise versions of **Security**.

On premise EBS will be deployed on **Security** with interfaces re-used and developed by the SGN integration team to keep existing data flows to and from the wider SGN systems landscape and external parties such as HMRC. SGN will procure the SaaS licences via a trade-in of the current perpetual licences of our EBS therefore restricting to annual cost to the current licence support costs.

All modules of the on premise **Security** modules with minimum changes applied. The following 13 modules are currently in use by SGN:

- iProcurement
- Projects
- Time and Labour Engine
- Human Resources
- Learning Management
- General Ledger
- Payables
- iSupplier Portal
- Purchasing
- Receivables
- Order Management
- Assets
- Cash Management

All SGN specific customisation existing in our current on-premise system will need to be either re-developed or removed in favour of new process adoption. A moderate cost has been put aside for these changes. There will new network connectivity required between SGN on premise or AWS infrastructure and a security federation will also be established between SGN single sign-on engine **Security**. There will be training required for the users of the new system where the process has changed but for large number of users it will just a change in URL address with limited to no training required.

SGN will make use of favourable licence conditions available from **Security** as one of our strategic partners for over a decade.

### SAP Cloud ERP migration summary:

The SAP Cloud ERP will be deployed with all new integrations developed by SGN integration team for moving data between our other front office systems. SGN will need to procure the SaaS licences for SAP Cloud ERP as new licences for every module (13) that currently exists in our current **Security**. The following **Security** currently are in use at SGN that will need to be replaced with same functionality modules in the SAP system:

- iProcurement
- Projects
- Time and Labour Engine
- Human Resources
- Learning Management
- General Ledger
- Payables
- iSupplier Portal
- Purchasing
- Receivables
- Order Management
- Assets
- Cash Management

The SAP Cloud ERP will be integrated with SGN single sign-on engine **Security** and all historical data will need to be transformed, transported and uploaded into the new system. Network and support system connectivity will need to be designed and implemented to the new cloud hosting locations.

Due to new system interfaces and processes, SGN's business will require a thorough change management strategy implementation along with training for all staff.

## 7.4 Options Cost Summary Table

**Security** cost summary:

The following table provides the cost breakdown for investment as in the preferred option of investing into migrating to **Security**.

Table 2: Cost breakdown for the preferred option.

Option	Template	Cost Breakdown	Total Cost (£m)
Replace Oracle EBS 12.2 with <b>Security</b>	IT Capex	Resources	3.60
		Software	0.41
		Hardware	
		Contingency	
		<b>Total</b>	<b>4</b>

Table 3: Cost breakdown by activity type for the preferred option.

Investment type	FY 2022	FY 2023	FY 2024	Totals
Architecture and design (£)	£25,000	£10,000	£10,000	£45,000
Data Governance (£)	£70,000	£20,000	£20,000	£110,000
Customisation and testing (£)	£600,000	£600,000	£600,000	£1,800,000
Project Management (£)	£160,000	£80,000	£80,000	£320,000
Data management (£)	£110,000	£20,000	£20,000	£150,000
Integration (£)	£180,000	£60,000	£60,000	£300,000
Software licences (£) (existing)	£125,000	£0	£0	£125,000

<b>Training and change management (£)</b>	£130,000	£30,000	£30,000	£190,000
<b>Supplier consultation (£)</b>	£600,000	£180,000	£180,000	£960,000.00
<b>Total capex investment (£M)</b>	<b>£2.00</b>	<b>£1.00</b>	<b>£1.00</b>	<b>£4.00</b>

SGN currently has perpetual software licences to **Security** with a recurring support cost paid out to **Security** annually. The subscription price received from **Security** matches the annual support cost currently paid for on premise EBS hence there is only a nominal increase in software licence price in the first year to cover for the transitional cost where the two systems might work in parallel before the cut over.

A significantly large part of the cost will be spent on customisation and testing, alongside supplier consultation and advice on change management and practices that may be required. The deployment of the system will be in phases, the focus of migration for the first year (FY 2022) would be on migrating the financial accounting modules covering the AR, AP, GL, statutory accounting books, MIS accounting books, order management, cash management, asset management, journal entries and the MIS. The second year will be focused on Procurement and HR modules, the final third year will be to move contractor and invoicing systems to the **Security** Cloud.

#### SAP Cloud ERP cost summary:

The following table provides the cost breakdown for investment as in the second option of investing to migrate on to **Security**.

Table 4: Cost breakdown for the second option.

Option	Template	Cost Breakdown	Total Cost (£m)	
<b>Replace</b>	<b>Security</b>	IT Capex	Resources	15.45
			Software	4.55
			Hardware	
			Contingency	
			<b>Total</b>	<b>20</b>

Table 5: Cost breakdown by activity type for the second option.

Investment type	FY 2022	FY 2023	FY 2024	FY 20242	FY 2025	Totals
<b>Architecture and design (£)</b>	£330,000	£330,000				£660,000
<b>Data Governance (£)</b>	£400,000	£400,000				£800,000
<b>Customisation and testing (£)</b>	£2,500,000	£2,500,000				£5,000,000
<b>Project Management (£)</b>	£420,000	£420,000				£840,000
<b>Data management (£)</b>	£450,000	£450,000				£900,000
<b>Integration (£)</b>	£900,000	£900,000				£1,800,000
<b>Software licences (£)</b>	£1,300,000	£1,500,000				£2,800,000
<b>Training and change management (£)</b>	£1,000,000	£500,000				£1,500,000
<b>Supplier consultation (£)</b>	£2,700,000	£3,000,000				£5,700,000
<b>Total capex investment (£M)</b>	<b>£10.00</b>	<b>£10.00</b>	<b>£0.00</b>	<b>£0.00</b>	<b>£0.00</b>	<b>£20.00</b>

Like any new ERP implementation, move to **Security** will start with requirements mapping, architecture, design and project planning. A new implementation will require an in-depth consultation with the SGN business on the impact with an end to end process mapping. New systems with new interfaces would require a complete re-think on SGN's data governance, data management, integration and training leading to significantly costs. A typical ERP implementation takes up to 2 years with a module wise rollout alongside tactical integrations to the old systems for the end to end processes to work. This results into a lot of additional sunk cost during the transition incurred through supplier consultations, customisations and testing.

New SaaS software licences will need to be procured and other systems, such as our front office systems, will be integrated on to the new platform over a course of next 3 years.

The cost estimations derived here are purely on the basis of SGN's experience of implementing our current **Security** systems in 2009/10.

## 8 Business Case Outline and Discussion

### 8.1 Key Business Case Drivers Description

SGN's licence to operate requires us to be compliant with legislative requirements (safety, reliability, affordability and environmental). The uniform network code and the supply point administration agreement also require SGN to work towards the improvement in these areas. It is critical that we can comply with legislation in regard to how we manage our operation on a daily basis. Investing in a supported, well maintained and integrated technology solutions, SGN will continue to provide operational and safety information to Regulatory bodies, Industry and Government. Our asset management, operations and safety management activities are key in our ability to operate in the most cost-effective way for our customers.

Failure to replace the unsupported **Security** back office system could result in SGN being unable to fulfil many of our obligations. SGN's licence to operate requires us to be compliant with legislative requirements (HMRC, SHE, employment law, procurement, accounts and reporting regulations). Failure to renew these systems could result in SGN being unable to pay staff, contractors and suppliers. The knock-on effect of this would be critical system and process failures potentially leading to failure in emergency standards, gas explosion and loss of life (£16m loss of life, up to £100m/10% of turnover fine, unlimited HSE Penalty).

The investment also underpins our ability to report and plan to meet our Regulatory Output Measures including our ability to respond to Emergencies as well as repair and replace our network efficiently.

SGN has developed and will continue to develop, people and process capabilities in back office operations to be able to leverage the technology in these areas. Our recent utilisation of **Security** ), and our investment in the integration and data flows with other supporting systems will provide a firm foundation to meet our future obligations and responsibilities as a GDN in GD2.

In addition to realising operation necessities associated with system replacement, SGN also needs capabilities for risk reduction in identifying potential exposure to our investments, operations and security. This is an essential investment for SGN to protect assets and services and to build defences against misuse in the future.

Table 6: Key value drivers in options analysis.

Option No.	Desc. of Option	Key Value Driver
1	Replace Security with Security	<ul style="list-style-type: none"> <li>Supported IT Systems</li> <li>Emergency Outputs Maintained</li> <li>Repair Outputs Maintained</li> <li>Risk Reduction Outputs Maintained</li> <li>Reliability Outputs Maintained</li> <li>Customer Outputs Maintained</li> </ul>
2	Replace Security with Security	Alternative to option 1 with a higher cost to implement, more complexity in integration and significant increase in annual support cost.

Table 7: Summary of CBA results.

NPVs based on Payback Periods (absolute, £m)								
Option No.	Desc. of Option	Preferred Option (Y/N)	Total Forecast Expenditure (£m)	Total NPV	2030	2035	2040	2050
Baseline	Do Nothing / Do minimum	N	0.00	-117.73	<b>-117.73</b>	<b>-117.73</b>	<b>-117.73</b>	<b>-117.73</b>
1	Option 1 <b>Absolute NPV</b>	Y	-4.00	-19.60	<b>-5.21</b>	<b>-7.74</b>	<b>-10.08</b>	<b>-14.07</b>
2	Option 2 <b>Absolute NPV</b>	N	-20.00	-67.05	<b>-19.92</b>	<b>-27.70</b>	<b>-37.51</b>	<b>-48.72</b>
1	Option 1 NPV <b>relative to Baseline</b>	Y	-4.00	-19.60	<b>112.52</b>	<b>109.99</b>	<b>107.65</b>	<b>103.66</b>
2	Option 2 NPV <b>Relative to Baseline</b>	N	-20.00	-67.05	<b>97.80</b>	<b>90.03</b>	<b>80.21</b>	<b>69.01</b>

**Key Assumptions:**

**Probability of fatalities / other societal cost:** SGN manage its IT estate in line with the HSEs ALARP (as low as reasonably practicable) risk management principles. On that basis SGN have assumed a failure to invest in required adoption of technology, replacement or refresh activity for safety critical systems, would lead to catastrophic system failure as well as a lack of 3rd party support (based on support contracts, 3rd party roadmaps, architectural standards and internal policies, designed to ensure upgrade, replacement or refresh activity is carried out at the appropriate point in time in order to prevent a non-recoverable functional, technical or security failure).

**Probability of fatalities / other societal cost:** SGN have assumed that a lack of investment combined with a lack of support into new technologies would prevent the reinstatement of systems should they fail.

**Probability of fatalities / other societal cost:** SGN have assumed a catastrophic failure of safety critical systems and an inability to reinstate systems after failure would lead to an inability to respond to gas emergencies, an inability to know where our assets are and an inability to track performance and regulatory outputs.

**Probability of fatalities / other societal cost:** SGN have assumed a catastrophic failure of safety critical systems that are on old technologies and an inability to reinstate systems after failure would

lead to an inability to respond to gas emergencies, an inability to know where our assets are and an inability to track performance and regulatory outputs.

**Probability of fatalities / other societal cost:** SGN have assumed an inability to respond to gas emergencies, an inability to know where our assets are and an inability to track performance and regulatory outputs would inevitably lead to a catastrophic incident e.g. explosion and loss of life (£17.73m). This assumption is supported by section 2 of the Health and Safety at work act which identifies scenarios that would result in loss of life.

**Probability of fatalities / other societal cost:** SGN have assumed an inability to respond to gas emergencies, an inability to know where our assets are and an inability to track performance and regulatory outputs would inevitably lead to an inability to operate. This would lead to a catastrophic breach of license conditions (up to £100m fine)

**Probability of fatalities / other societal cost:** SGN have assumed catastrophic failures in regard to loss of life (£17.73m), a breach of license conditions (up to £100m) and/or a breach of GDPR legislation (up to £40m) will occur within a year of failing to adhere to support contracts, 3rd party roadmaps, architectural standards and internal policies designed to ensure upgrade, replacement or refresh activity is carried out at the appropriate point in time to in order to prevent a non-recoverable functional, technical or security failure

**Capex & Opex expenditure:** Assumes a steady rollout, throughout GD2, across industry of Open Data Sharing and whole energy system approach - i.e. Ofgem and BEIS policy does not require accelerated delivery of open data and energy system approach

**Capex & Opex expenditure:** Assumes shared investment of establishment and operation Open Data Sharing service

**Capex & Opex expenditure:** Assumes "reasonable endeavors" for service elements: quality of data, frequency of service delivery, service SLA's etc.

**Capex & Opex expenditure:** Assumes little to no requirement for specific technology solutions within SGN to support industry Open Data service, which are not aligned to our technology policies and roadmaps

## 8.2 Business Case Summary

This engineering justification considers the option 1 of investing in the areas required to deliver SGN's GD2 plans. The other options available add significant risks and costs to SGN's overall plans and obligations as a Gas Network that are captured in sections above.

The summary of the cost benefit analysis is presented as below:

Table 8: Business case matrix.

	Replace	Security	Replace	Security
				ERP
GD2 Capex (£m)		4.00		20.00
Number of Interventions		3.00		2.00
Carbon Savings ktCO2e (GD2)		0.00		0.00
Carbon Savings ktCO2e /yr		0.00		0.00
Carbon Emission Savings (35yr PV, £m)		0.00		0.00
Other Environmental Savings (35yr PV, £m)		0.00		0.00
Safety Benefits (35yr PV, £m)		17.73		17.73
Other Benefits (35yr PV, £m)		100.00		100.00
Direct Costs (35yr PV, £m)		-15.86		-55.64

NPV (35yr PV, £m)	101.87	62.09
<b>High Carbon Scenario</b>		
Carbon Emission Savings (35yr PV, £m)	0.00	0.00
High Carbon NPV (35yr PV, £m)	101.87	62.09

## 9 Preferred Option Scope and Project Plan

### 9.1 Preferred option

This engineering justification recommends the option of investing in the areas required to deliver SGN's GD2 plans. The alternative investment plan as shown in the second option does not provide any significant advantage but is significantly higher in cost.

The investment listed above relate to accepting, adopting and benefitting from the minimum, mandatory investment required to continue to operate. Failure to undertake this investment will ultimately result in SGN being unable to meet its obligations as a Gas Network operator.

SGN's proposal is to spend a total of £4 Million over a 3 years period starting from 2022 on our existing technology that we and industry experts consider to be essential to run and maintain a safe, reliable and affordable gas network.

### 9.2 Asset Health Spend Profile

SGN plans to invest up to £4 million on replacing our back-office systems in the first three years of the GD2 commitments. This will be a project driven capex investment

Table 9: Asset health spend profile.

Asset Health Spend Profile (£m)						
	2021/22	2022/23	2023/24	2024/25	2025/26	Post GD2
with <b>Security Security</b>	2.00	1.00	1.00	0.00	0.00	Spend profile continues post GD2

The investment for financial planning and reporting tool will be based on the procurement of technology, such as **Security**, and the delivery framework including design and architecture. The procurement will also include data and integration tools, consulting for specialist software & data scientist skills required to design, implement and maintain the solutions. The cost also includes the project management and technology skill hiring and/or development costs consisting of internal staff, contractors and specialists to deliver the business outcomes. The cost for training and business change management, travel associated with the project delivery and engineering costs required for on field changes will also be included in the investment costs.

Along with the project costs, that will largely be capitalised, there will an ongoing opex cost required to run, maintain and replace the devices/software from time to time that will be part of the overall opex costs covered in our plans.

### 9.3 Investment Risk Discussion

As part of annual operating planning process, SGN management will study and prioritise the use cases for the proposed yearly investments every year to align these planned investments and to optimise these. Thus, ensuring maximum efficiency and benefit to customers. All expenditure listed in this paper will be defined, monitored, controlled and reported on a periodic basis in line with the corporate governance, legal, regulatory and financial reporting obligations that apply to SGN and all GDNs.

At a high-level planning perspective, we have assumed a steady state, phased approach to investment in the first three year with higher first year cost related to migration of the largest number of system modules in the first year as part of the core finance platform.

The key risk associated with the proposed option is on data transition and user training. SGN will mitigate these through our structured approach to data governance and compliance, as well as using our tried and tested project delivery methodology to deliver change programmes.

Table 10: Risk Matrix

Risk Description	Impact	Likelihood	Mitigation/Controls	Comments
Change in capital expenditure	Capex expenditure	<=20%	Thorough Project Management, design and testing, risk and issue management. Appropriate budget assigned for delivery considering lessons learnt from previous upgrades.	The upgrade may upgrade our ability to run critical payroll and finance processes. This could result in further system releases and associated testing leading to additional cost.
Change in scope and capital expenditure	Capex expenditure	>40% & <=60%	We are discussing the next steps for a more detailed assessment with Oracle.	Oracle have done an initial expert assessment however it was high level and there is a risk that the proposed scope and associated cost may change.
Change in scope, capital expenditure and timelines	Capex expenditure	>40% & <=60%	Investment in technology roadmaps, ensuring early sight of any changes.	Changing technology trends including operating systems and applications impact the cost and timelines for delivery of the option.

#### CAPEX Sensitivity:

A sensitivity-based risk analysis was performed with a mid-level sensitivity applied to the investment plan. The impact on the plan based on the three sensitivity levels is presented in the table below as a reference.

Table 11: Sensitivity risk analysis.

	Low	Mid	High
GD2 Capex (£m)	4.00	4.00	6.00
Number of Interventions	3	3	3
Carbon Savings ktCO2e (GD2)	-	-	-
Carbon Savings ktCO2e /yr	0	0	0
Carbon Emission Savings (35yr PV, £m)	0.0	0.0	0.0
Other Environmental Savings (35yr PV, £m)	0	0	0
Safety Benefits (35yr PV, £m)	3.5	17.7	17.7
Other Benefits (35yr PV, £m)	20.0	100.0	100.0
Direct Costs (35yr PV, £m)	-15.9	-15.9	-23.8
NPV (35yr PV, £m)	7.7	101.9	93.9

We believe the preferred option is for keeping up with technology advancement. For sensitivity analysis, the following has been applied to the preferred option of pre-emptive replacement:

**Low Case:** SGN have applied an 80% reduction has been applied to the Safety Benefits associated with the risk of a fatality and Other Benefits associated with the impact of a Breach of Licence Conditions.

**Mid Case:** no changes have been applied, this is the expected output required for the GD2 time period.

**High Case:** SGN have applied an additional 50% on the CAPEX and OPEX expenditure, as this is believed to be the potential cost increase if SGN do not go to tender and achieve best possible market prices. This could also be impacted by political changes which may impact on resource availability or material costs. This increase in cost also allows for any issues in obtaining generic designs for the full volume of works or SGN not being able to deliver these projects efficiently due to internal processes which would increase contract labour costs.

Project payback has not been carried out as part of this analysis due to the effect of the Spackman approach. For a cash-flow traditional project payback period please see scenario 4 of our Capitalisation Sensitivity table.

### Capitalisation Rate Sensitivity

Consumers fund our Totex in two ways – opex is charged immediately though bills (fast money – no capitalisation) and capex / repex is funded by bills over 45 years (slow money – 100% capitalisation). The amount deferred over 45 years represents the capitalisation rate. Traditionally in ‘project’ CBA’s the cashflows are shown as they are incurred (with the investment up front which essentially is a zero capitalisation rate). Therefore, we have developed scenarios that reflect both ways of looking at the investment – from a consumer and a ‘project’.

The scenarios are summarised as follows:

- Scenario 1 - we have used the blended average of 65%, used in previous iterations of this analysis.
- Scenario 2 - we have represented the Capex and Opex blend for the two networks, as per guidance.
- Scenario 3 - addresses our concerns on capitalisation rates whereby Repex and Capex spend is deferred (100% capitalisation rate) and Opex is paid for upfront (0% capitalisation rate).
- Scenario 4 - this reflects the payback period in 'project' / cash-flow terms and provides a project payback.

We have taken a view of the NPV in each of the scenarios, except for scenario 4, at the 20, 35 and 45 Year points, to demonstrate the effect of Capitalisation Rate on this value.

Table 12: Capitalisation rate sensitivity

Scenario	1	2 SGN	3	4
Capex (%)	65	41	100	0
Opex (%)	65	41	0	0
Repex (%)	100	100	100	0
<b>Output</b>				
NPV (20yr PV, £m)	108.64	107.46	110.35	
NPV (35yr PV, £m)	102.70	101.87	103.91	
NPV (45yr PV, £m)	99.78	99.20	100.63	
Payback	3.00	3.00	3.00	3.00

## Appendix A - Acronyms

Acronym	Description
AWS	Amazon Web Services
CEG	Customer Engagement Group
EBS	E-Business Suite
ERP	Enterprise Resource Planning
GDPR	General Data Protection Regulation
SAAS	Software as a Service
SAP	Software company SAP (Systems, Applications, Products)
SGN	Scotia Gas Network