RIIO GD2 Business Plan Appendix

IT and Cyber Resilience

December 2019 submission

Your gas. Our network.

www.sgn.co.uk

Contents

1 Overview

Scope of this appendix

This appendix covers all Information Technology (IT) related investment including the provision of standard services and the investment required to provide resilience to a changing level of cyber security threats that are expected to continue to evolve over the course of the GD2 period.

All elements of the outcomes and outputs defined within the broader business plan are underpinned by the IT expenditure defined within this paper. There are particular overlaps with the E&I appendix, operations and the deployment of innovation.

Impact

Our safety, operational, stakeholder and customer service performance defined within the business plan, can and will only be achieved with the investment in and provision of IT as described within this appendix.

This plan, therefore, covers the minimal investment required to deliver a safe and reliable network and associated operations.

We have also identified additional, stakeholder-led, requirements and outputs which can be considered as part of the GD2 plan. These requirements and associated costs are included within the total costs presented and relate specifically to open data provision and Data Communication Company membership. These outputs are in response to specific guidance and stakeholder requirements relating to digitalisation and smart meter data utilisation respectively. Our wider digitalisation ambition is defined under a separate strategy document and published on our website as requested by Ofgem.

Approach to GD2

Our IT expenditure and cost efficiency over the entire GD1 period is proven as being ‘best in class’ as defined by Gartner standards and definitions. This means our IT cost base is between the lower 25th percentile and the average cost base when compared with like-for-like peers i.e. UK asset-based utilities.

We have provided a separate, very detailed and independent cost assessment report from Gartner[1]. In addition to a detailed cost assessment of historical spend, this assessment has also provided an independent review of all future investment and associated costs.

The five-year IT cost profile defined in this plan has been based, in part, on GD1 expenditure but in particular the latter years of GD1. This is due to the levels and rate of change experienced in technology within our sector and indeed across all sectors. Comparing IT costs and expenditure from 2021 to 2026 to the cost expenditure in 2013 or across the earlier part of the GD1 period has limited relevance given the significant and fundamental changes which have occurred and will continue to occur in information and digital technology.

We have therefore based our planning and supporting analysis on our IT costs as at 2018/19 and the previous two years.

Future spend profiles in IT, in particular when considering technology spend beyond 2023, requires expert advice. Consequently, we have sought and utilised extensive advice and assurance from independent technology advisors as well as trusted partners, to inform the technology trends and spend profiles required throughout the GD2 period in particular, in the latter stages. These references are included later within this report.

[1] Gartner IT Cost and Capital Investment Assessment Project Report v1.2 15 March 2019

The RIIO-GD1 experience driving our GD2 plans

During GD1, three major shifts in technology occurred within our company and across all industries and these trends (plus others referred to later in this report) are reflected in both our historical and future plans:

- **Exponential growth in cyber threat.** Perhaps the most significant shift affecting our business and our stakeholders has been the exponential rise in the risk of a Cyber-attack globally, and in particular within the UK utilities and energy networks sector. This risk has a consequential impact on day-to-day operations and our ability to keep the gas flowing safely and reliably. In financial terms, when comparing the GD1 allowances in 2013 to our actual expenditure in 18/19, we have increased expenditure 40% year-on-year. This increased expenditure which is significantly above allowances, is further reflected in our commitment to Ofgem that an additional £16m would be spent on security (physical and cyber), over and above the allowances provided under GD1 as a part of our voluntary contribution. This contribution has been delivered in part by our ongoing cyber security programme and added to via our 'all in' migration to a cloud to drive improved security, our investment in new, secure cloud networking connectivity and the implementation of a new, managed security service provider bringing a significantly higher level of security management capability for us. Cyber security has become a government led requirement on our business. For this reason, a separate section within this report has been devoted to this topic to highlight the significant and substantive stakeholder demands on our cyber security capability.
- **Cloud based IT.** A shift from traditional 'on-premise', capital intensive IT infrastructure to the adoption of Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) cloud-based services. We have been at the forefront of the shift to cloud-based service adoption. During GD1, we have undertaken a major programme of work to migrate the majority of our IT services from on premise data centres manged and run on our behalf by SSE, to AWS public cloud. This programme is nearing completion and due to finalise the remaining service migrations at the end of financial year 2019/20. Additionally, we have migrated or introduced a number of PaaS and SaaS services e.g. Kony mobile development platform, Clickschedule SaaS and all of our productivity services have now been migrated to Microsoft O365. This migration from traditional on-premise based services to cloud has delivered our key stakeholder needs around:
  - Availability and resilience;
  - Increasing agility to respond to changing and increasing customer needs;
  - Significantly increased cyber security capability; and
  - More precise allocation of services to user needs through the ability to effectively turn services on and off at the point of use.
- **Increasing stakeholder, customer and employee demands in the use of digital technology.** During GD1 we have seen a significant shift in the expectations of employees and customers when it comes to how they interact with us and the use of technology to do so. 78% of our stakeholders expect us to utilise the latest technology[2] yet in the same research, only 38% of our stakeholders believe we are performing well or excelling in utilising the latest technology.

  We also know from our stakeholders, expectation on what constitutes 'good' customer service continues to rise, and more and more customers expect better communication on our work and how we affect their daily lives. Improved customer service is highly dependent on utilising the digital channels that are now part of our daily lives and our best in class customer satisfaction is more dependent on digital technology than ever before. Services such as 'live chat' which we introduced in 2017/18 on our website has become a standard mechanism for customers to communicate with companies and our ability to respond to and provide customer communication through digital social media channels such as Twitter and Facebook have become a basic expectation from most of our customers. We have also introduced platforms such as

‘CitNow’ which provides customers with a video message showing work done as part of our connections service. This type of service did not exist at the beginning of GD1 and, again, has become a standard means of communicating with customers across many other sectors. While we cannot be prescriptive around the expectations of customers to interact digitally over the rest of GD1 and throughout GD2, we know that trends such as in-home assistants, and voice activated digital interaction will require us and all GDNs to continue ensuring our services keep pace with customer demands.

In addition to this shift in customer expectations, all employees expect significantly different and new technology services to those that were available at the beginning of GD1. During GD1 we have seen the enormous societal and workplace shift through the adoption of mobile technology. This is demonstrated when considering that at the beginning of GD1, no field-based employee in our businesses utilised a smart phone or tablet device. Our company utilised one, basic, mobile data capture tool provided on a standard laptop. Mobile communication and the running of numerous mobile based applications for every single employee is now the norm and an essential part of the tools and equipment our workforce need to do their jobs safely, efficiently and effectively.

Finally, due to the major challenges associated with energy transition, towards the latter part of GD1, we have seen increasing expectations, requirements and opportunity to digitalise energy data for benefit of society as a whole. This is best encapsulated within the recommendations of the Energy Data Taskforce which is summary, highlights the need for the energy industry to:

- Drive the digitalisation of the energy system;
- Maximising the value and visibility of data; and
- Coordinate and make visible energy infrastructure assets.

Therefore, our GD2 plans reflect the mechanisms to enable further digitalisation and data sharing.

The GD1 experience has led to the following factors being incorporated within our GD2 business plan and associated costs:

- Cyber security expenditure increases in line with GD1 growth and increased risk, regulatory and legislative demands;
- Like for like investment in Customer satisfaction to keep pace with customer expectations;
- Increasing employee expectations and technology use in line with GD1;
- Future technology adoption to support Network management and Energy Resilience. The Increaseddemand, adoption and usage of Industrial Internet of Things (IIoT), Analytics and Data use, Machine Learning and Artificial Intelligence. This is required to support both continued resilience and network management levels and to lay the foundations to support a more complex energy system transition;
- Cloud: Movement from traditional capex investment in infrastructure to consumption based Opex costs; and
- Digitalisation and data sharing to support the UK’s energy transition.

This appendix and our Gartner costs assessment and assurance provides the evidence and accompanying stakeholder feedback to support these cost categories and levels of spend. We have defined each investment area in significant detail within individual engineering justification papers and cost benefit analyses.

Capital and operational expenditure differences

Historically, IT investment was easily and simply split between ‘Build’ and ‘Run’ with each type of spend falling solely into capital and operational expenditure (capex and opex) respectively. ‘Run’ involves the day-to-day IT operational environment and keeping existing IT services running; ‘Build’ costs historically, would have related solely to capital project expenditure.

It is important to note that due to the global trend of adopting Cloud based technologies that the historical split between opex and capex is no longer the same as it was. This is due to the accounting practices relating to Cloud expenditure (which will vary between companies) which, in simple terms, can result in what would have historically been ‘Build’, and hence capex, now being treated as opex. Equally, if prepaid commitment is made to Cloud service providers, depending on the terms, this can result in ‘Run’ costs which would have historically been treated as opex, now being treated as a capital asset.

For this reason, and to aid visibility and comparison of total expenditure (totex), the IT plan is a singular plan covering both capital and operational expenditure together. We have shown the plan in terms of ‘Run’ and ‘Investment’ costs and have also provided the financial split between capex and opex but as stated above, these are no longer the same definitions as was the case in the earlier part of GD1 and the GD1 price control allowances.

To maximise operational effectiveness, we provide a single set of IT services to both our Scotland and Southern networks. Therefore, in the context of the IT plan and cost assessment, both networks are incorporated.

IT, business IT, security and cyber resiliance

In a similar way to how opex and capex lines have become blurred, with the move towards cloud-based services the distinction between IT based and cyber security related costs can be equally hard to differentiate and are by definition, inextricably linked. For these reasons we have kept the two linked in this appendix. However, as part of our engagement with Ofgem and subsequent guidance, we have submitted a separate Cyber Resilience Business plan data template relating solely to operational technology security.

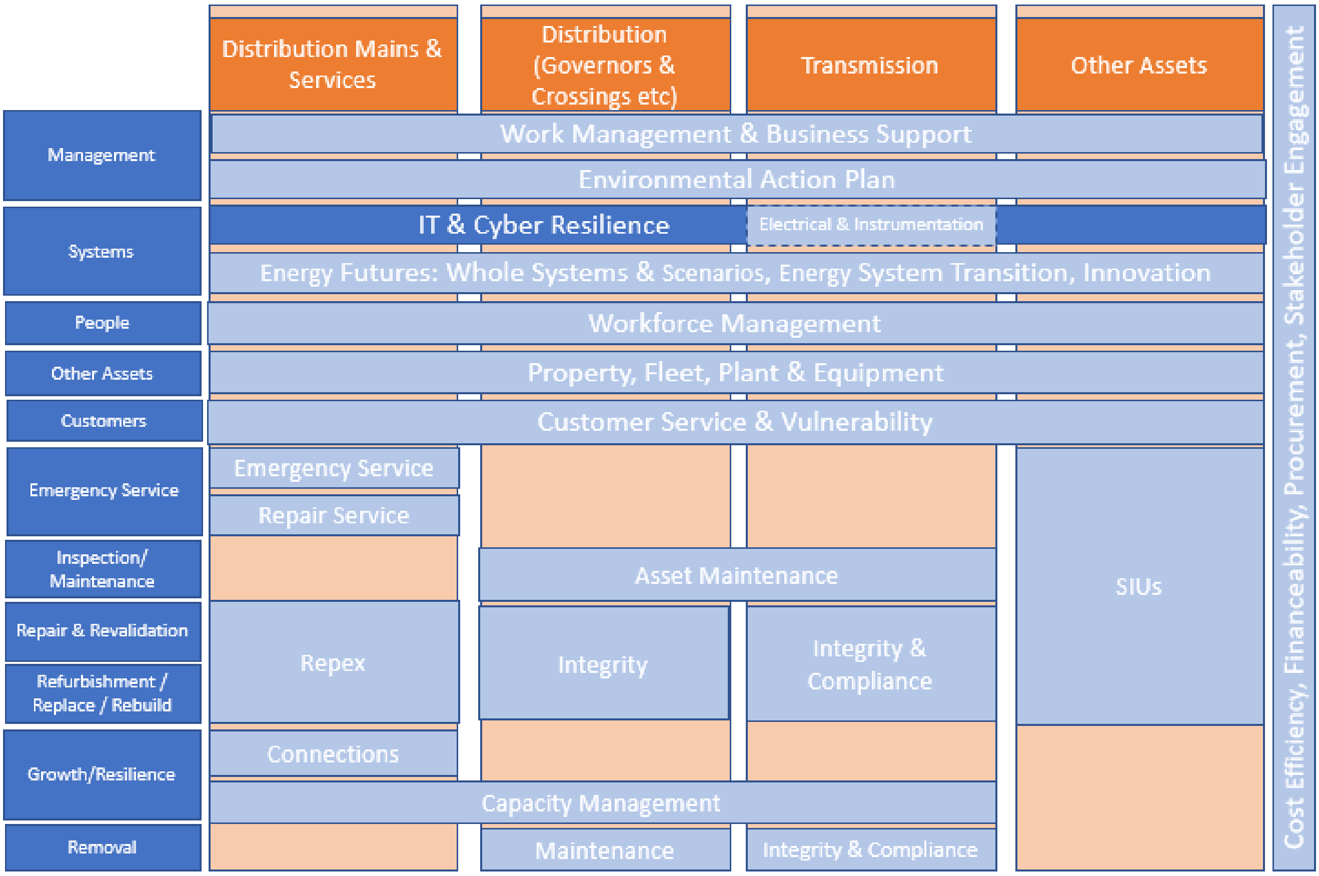
Table 1: IT costs (capex and opex costs)

IT capex costs (investment/projects only)													
SGN (£m)	**13/14**	**14/15**	**15/16**	**16/17**	**17/18**	**18/19**	**19/20**	**20/21**	**21/22**	**22/23**	**23/24**	**24/25**	**25/26**
Mandatory IT	13.12	23	13.07	7.01	16.33	13.08	11.59	4.94	9.40	9.25	9.36	7.83	7.11
Mandatory business	-	-	-	-	-	-	-	-	0.25	0.25	0.25	0.25	0.25
Business IT security	-	-	-	-	-	-	-	-	1.85	2.16	1.45	3.04	3.65
Cyber resilience	-	-	-	-	-	-	-	-	0.21	0.24	1.39	0.34	0.41
Future technology readiness	-	-	-	-	-	-	-	-	1.82	1.50	1.55	1.94	2.99
DCC membership	-	-	-	-	-	-	-	-	0.50	0.50	1.50	1.50	1.00
Open data	-	-	-	-	-	-	-	-	1.00	0.75	0.75	0.50	0.75
Total capex	**13.12**	**23.00**	**13.07**	**7.01**	**16.33**	**13.08**	**11.59**	**4.94**	**15.03**	**14.66**	**16.25**	**15.40**	**16.16**
IT opex costs (Run and investment)													
Mandatory IT	-	-	-	-	-	-	-	-	0.50	0.25	0.50	0.25	0.25
Mandatory Business	-	-	-	-	-	-	-	-	0.25	0.25	0.25	0.25	0.25
Investment run	-	-	-	-	-	-	-	-	0.98	2.37	3.70	4.96	6.30
Business IT security	-	-	-	-	-	-	-	-	0.43	0.59	1.30	1.62	2.03
Cyber resilience	-	-	-	-	-	-	-	-	0.50	0.57	0.14	0.18	0.23
Future technology readiness	-	-	-	-	-	-	-	-	0.10	0.10	0.20	0.50	0.60
DCC membership	-	-	-	-	-	-	-	-	0.10	0.10	0.10	0.10	0.10
Open data	-	-	-	-	-	-	-	-	0.30	0.30	0.30	0.30	0.30
Licencing	-	-	-	-	-	-	-	-	0.40	0.40	0.40	0.40	0.40
Ongoing cost	21.16	22.62	24.09	27.33	27.66	36.9	33.09	29.23	21.64	22.26	22.26	22.26	22.26
Total opex	**21.16**	**22.62**	**24.09**	**27.33**	**27.66**	**36.90**	**33.09**	**29.23**	**31.75**	**33.74**	**35.71**	**37.38**	**39.27**

Changes in cost phasing and our profile of costs are defined in section 6.6.

2 IT and cyber resilience within the business plan

Figure 1: Identifies our business plan appendix structure



Distribution Mains & Services
Distribution (Governors & Crossings etc)
Transmission
Other Assets
Management
Work Management & Business Support
Environmental Action Plan
Systems
IT & Cyber Resilience
Electrical & Instrumentation
Energy Futures: Whole Systems & Scenarios, Energy System Transition, Innovation
People
Workforce Management
Other Assets
Property, Fleet, Plant & Equipment
Customers
Customer Service & Vulnerability
Emergency Service
Emergency Service
Repair Service
Inspection/ Maintenance
Asset Maintenance
SIUs
Repair & Revalidation
Repex
Integrity
Integrity & Compliance
Refurbishment / Replace / Rebuild
Growth/Resilience
Connections
Capacity Management
Removal
Maintenance
Integrity & Compliance
Cost Efficiency, Financeability, Procurement, Stakeholder Engagement

In this appendix we have set out our investment against allowances in GD1 for IT & Cyber resilience, and the investment that we are proposing to undertake in GD2 which, as can be seen from the Figure, impact across the whole of our asset base.

3 GD1 performance and learning

The performance of our IT systems has underpinned and enabled all outputs and operational performance described in our business plan and reported each year through our regulatory reporting mechanism. Without the historical investment in the IT that supports our business, and everything we do, the levels of safety, resilience and customer satisfaction would not have been met.

Levels of IT expenditure during GD1 has been independently assessed and evaluated in significant detail by an independent and globally recognised technology research and advisory company called Gartner. Gartner have assessed our IT costs against like for like companies i.e. UK asset-based utilities[19].

Throughout GD1, we have demonstrated 'best in class' cost efficiency. This means our IT expenditure falls between the lower 25th percentile and the 50th percentile when compared to peers. This is within the context of providing globally leading IT services as demonstrated in our advisory papers provided as supporting evidence with our final business plan submission.

Based on the detailed benchmarking and analysis, the Gartner assessment has concluded:

- Our historic spend across GD1 as a percentage of revenue is between the peer average and 25th percentile. At 3.34% it is 16% lower than the comparable industry peer average;
- Our BAU IT spend (opex and depreciation) is £1.8m less than the average spend of comparable technology peers;
- Some service level targets are more stringent in comparison to industry standards;
- Our IT Spend per Employee, at £12,017 a year, is 3.4% lower than the peer average of £12,435; placing it within the 'best in class' category of cost efficiency; and
- Our GD2 Investment planning and provision estimates are within the target Gartner equivalent range.

It should be noted that the information and cost data assessed as part of the detailed benchmarking was derived from data supplied for the financial year 2018/19. This was our highest year of spend in GD1 to-date, due to our cloud investment and double running of services whilst we have been transitioning from our on-premise data centres and service providers to our new public cloud provider and associated services and suppliers.

Despite this investment spike and dual running costs, we have still demonstrated cost efficiency levels on a par with the peer average as confirmed by the assessment. In the year 2018/19 our total IT budget (opex and capex) is 2.8% higher than the average of comparable industry peers. If the one-off investment in dual running costs and the cloud programme are removed, our IT budget is lower by 4.5%.

3.1 Legislative Background

We are licenced to transport gas in our two distribution networks through the Gas Act 1986 and are required to operate and maintain a safe and reliable network for supply of gas to all our 5.9 million customers during the most severe of winter conditions when gas demands typically reach peak levels.

As noted above, all elements of the outcomes and outputs defined within the broader business plan are underpinned by the IT expenditure defined here. Failure to meet these outcomes and outputs could result in critical system and process failures potentially leading to failure of emergency gas escape response standards, gas explosion and loss of life (£17.3m loss of life cost and up to £100m/10% turnover fine, and unlimited HSE penalty).

In addition to this, any failure relating to data loss under GDPR and/or the service availability failure as a result of Cyber Security failings as defined under Network Information Systems Directive, could result in fines of up to 4% of turnover which equates to approximately £40m in each case).

3.2 Output delivery

We have consistently provided globally best in class solutions and services to our customers and employees. Detailed evidence has been provided within an independent assurance report[19] and advisory papers which are summarised in appendix 2 of this paper. This assurance report and accompanying advisory papers demonstrate that we have been able to deliver world-leading services whilst maintaining sector leading cost efficiency. In summary, we can demonstrate that across our asset base we have invested in some of the best IT platforms and services that are available globally whilst keeping costs down. A sample of these best in class services are:

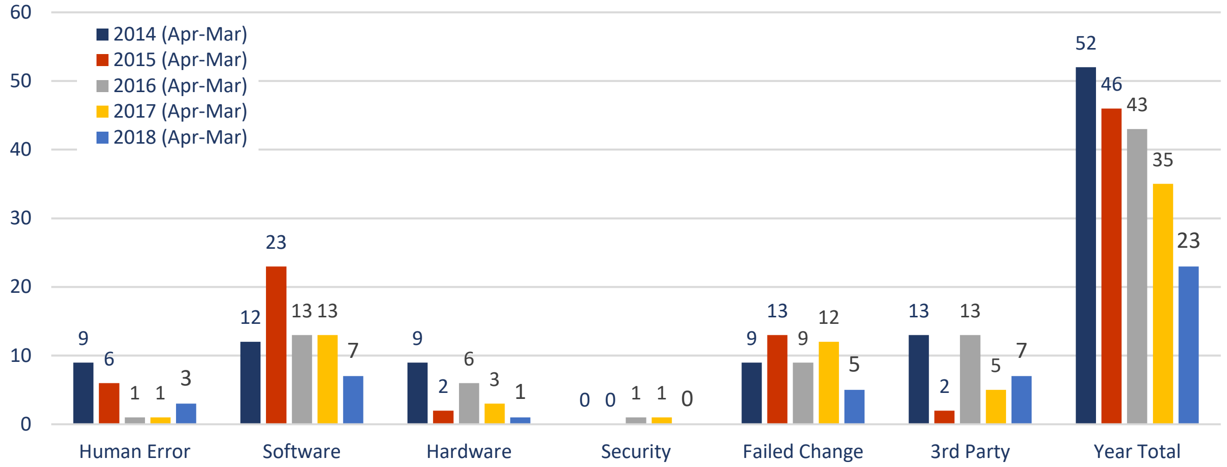
- Public Cloud - Our investment and wholescale migration to Amazon Web Service, (AWS), who provide the best public cloud infrastructure globally;
- Managed workplaces - Our Fujitsu managed service is globally best in class compared to all other service providers;
- Asset Management - Our Maximo asset management platform continues to be the best possible asset management solution available on the market. Significantly ahead of all other competitors;
- Field Service Management and Workforce Scheduling - Our ClickSoftware scheduling solution is also world leading;
- Mobile Development - In GD1, we invested and implemented one of the leading mobile application development platforms called Kony. This has been instrumental in providing solutions to enable our industry leading gas customer service levels;
- Analytics and Business Intelligence - In GD1 we put in place a high-quality Analytics and BI platform, Tableau. This world leading service enables us to capture and report on our primary outputs as well as ensure our business has the insight and information to meet all its licence and statutory responsibilities; and
- Security Operations and Incident and Event Monitoring - In 2018, SGN implemented a new and significantly improved managed security service utilising leading security services from Symantec and Fujitsu and supported by numerous security tools and products required to manage cyber security risk across our IT estate.

In addition to demonstrating 'Best in Class' Cost efficiency, throughout GD1 our peer comparison analysis and benchmarking report[1] has demonstrated that in most areas, we have operated and provided service levels that are either on a par with or more stringent than the peer average. Our availability standards are higher.

The continued investment in our estate as outlined above and within the sample advisory papers provided as supporting evidence with our business plan, has enabled continuous delivery and year on year improvement in the IT services we provide. In GD1 we have consistently improved the quality of our IT operational services by reducing IT outages and incidents year on year as shown below in figure 2. This level of service is fundamental to our business having delivered the outputs and outcomes during GD1 while ensuring our gas customers receive the best service in our industry.

Our GD2 plan and costs are based on maintaining the service levels and outcomes outlined below. Reduced expenditure in any of these areas will have a consequential impact on the associated business outcome.

Figure 2: IT incident analysis, number of Priority 1 incidents by year



NB

Priority 1 is defined as a complete loss of a specific IT service

Primary outputs and IT deliverables

Output area	Output Name	Output target	IT Standards of Service	GD1 Deliverables	Proposed GD2 Deliverables
Safety	Emergency	Attend >=97% of uncontrolled PREs within 1hr	IT availability standards for critical systems (99.5%), device replacement within 1 working day, incident response SLAs e.g. P1 incident response within 4 hours for critical systems, cyber incident response SLAs, vulnerability and patch management policy, architectural principles and security standards.	Front Office service provision (Maximo Work and Asset Management, ESRI Geospatial Asset Management, Click/Field Service Edge Scheduling, Agentry Work Management and Data Capture, Geofield Geospatial Data Capture, Digital Asset Maps, Insight Streetworks Management, Clearman Reinstatement Management), Cognos and Tableau Reporting service provison, Back Office service provision (Oracle EBS, CIPS Contractor payment system), system and infrastructure upgrades, support and maintenance.	Telemetry Refresh, Control Room Replacement or Redesign, BAU Capex, Front Office Replacement or Redesign, Network and Communications Refresh, Device Refresh, Data Governance and Quality, Regulatory and Mandatory Change, Cyber Security Investment, Integration Replacement, Non Core Application Refresh, Back Office Replacement or Redesign, Financial Planning and Reporting, Future Technology Readiness (IIOT, Data and Analytics)
		Attend >=97% of controlled PREs within 2hr			
	Repair	Accumulated annual end of day repair risk <= 2012/13 base			
		Proportion of gas escapes prevented within 12 hrs > 60%			
	Major Accident Hazard Prevention	Annual acceptance of Safety Case		O365 and productivity service provision, MHUB Policy service provision, Cognos and Tableau Reporting service provision, MOBI Inspector service provision, system upgrades, support and maintenance.	
		COMAH report reviewed by HSE			
	Iron Mains risk removed	Cumulative iron mains 'off-risk' >= GD1 baseline by 2021		Front Office service provision (Maximo Work and Asset Management, ESRI Geospatial Asset Management, Click/Field Service Edge Scheduling, Agentry Work Management and Data Capture, Geofield Geospatial Data Capture, Digital Asset Maps, Insight Streetworks Management, Clearman Reinstatement Management), Back Office service provision (Oracle EBS, CIPS Contractor payment system), Cognos and Tableau Reporting service provision, Mains Risk Replacement System Service Provision (MRPS), system and infrastructure upgrades, support and maintenance.	

Reliability	Loss of supply	Management of number of interrupt's and duration by cause such that volume and duration <= baseline by 2021.	IT availability standards for critical systems (99.5% Front Office, 99.95% SCADA and Telemetry), device replacement within 1 working day, incident response SLAs e.g. P1 incident response within 4 hours for critical systems, cyber incident response SLAs, vulnerability and patch management policy, architectural principles and security standards.	SCADA and Telemetry High Pressure Network Control and Monitoring service provison, Demand Management service provision, TIme to Fail service provision, Front Office service provision (Maximo Work and Asset Management, ESRI Geospatial Asset Management, Click/Field Service Edge Scheduling, Agentry Work Management and Data Capture, Geofield Geospatial Data Capture, Digital Asset Maps), Back Office service provision (Oracle EBS, CIPS Contractor payment system), Cognos and Tableau reporting service provision, system and infrastructure upgrades, support and maintenance.	Telemetry Refresh, Control Room Replacement or Redesign, BAU Capex, Front Office Replacement or Redesign, Network and Communications Refresh, Device Refresh, Data Governance and Quality, Regulatory and Mandatory Change, Cyber Security Investment, Integration Replacement, Non Core Application Refresh, Back Office Replacement or Redesign, Financial Planning and Reporting, Future Technology Readiness (IIOT, Data and Analytics)
	Network reliability	Maintaining Operational Performance Achieved through secondary deliverables: Controlled reduction in 'fault hrs per site' and 'PSSR faults per site' <= 2021 target. Elimination of 'Off-take metering errors'.		SCADA and Telemetry High Pressure Network Control and Monitoring service provison, PMAC Pressure Management service provision, Front Office service provision (Maximo Work and Asset Management, ESRI Geospatial Asset Management, Click/Field Service Edge Scheduling, Agentry Work Management and Data Capture, Geofield Geospatial Data Capture, Digital Asset Maps), Cognos and Tabeau reporting service provision, Lotus Notes Logbook service provision, Alarm Response System service provision, High Pressure Management Gas Quality Information System (HPMIS) service provision, 3rd Party Connection Management (SQS) service provision, system and infrastructure upgrades, support and maintenance.	
	Network capacity	Achieving 1:20 obligation Delivered through secondary deliverables: 'Utilisation' of capacity at DN sites does not exceed 'post investment' parameters.		Synergi Gas Low Pressure Modelling service provison, Falcon High Pressure Modelling service provision, Demand Derivation Modelling service provision, Synergi Forecaster High Pressure Modelling service provision, Cognos and Tableau reporting service provision, system and infrastructure upgrades, support and maintenance.	

Social	Carbon Monoxide Awareness	Increase in stakeholder awareness of CO risks (as measured relative to baseline survey).	IT availability standards for critical systems (99.5%), device replacement within 1 working day, incident response SLAs e.g. P1 incident response within 4 hours for critical systems, cyber incident response SLAs, vulnerability and patch management policy, architectural principles and security standards.	O365 and Productivity service provision, Stakeholder Relationship Management Database service provision, SGN Website service provision, Social Media Tooling service provision, Cognos and Tableau reporting service provision, system and infrastructure upgrades, support and maintenance.	BAU Capex, Front Office Replacement or Redesign, Network and Communications Refresh, Device Refresh, Data Governance and Quality, Cyber Security Investment, Back Office Replacement or Redesign, Financial Planning and Reporting
	Fuel Poor connx	Reduce fuel poverty through the connection of 20,000 households to the gas network by 2021.		Front Office service provision (Front Office service provision (Maximo Work and Asset Management, ESRI Geospatial Asset Management), Cognos and Tableau reporting service provision, Back Office service provision (Oracle EBS, CIPS Contractor payment system), O365 and productivity service provision, system and infrastructure upgrades, support and maintenance.	

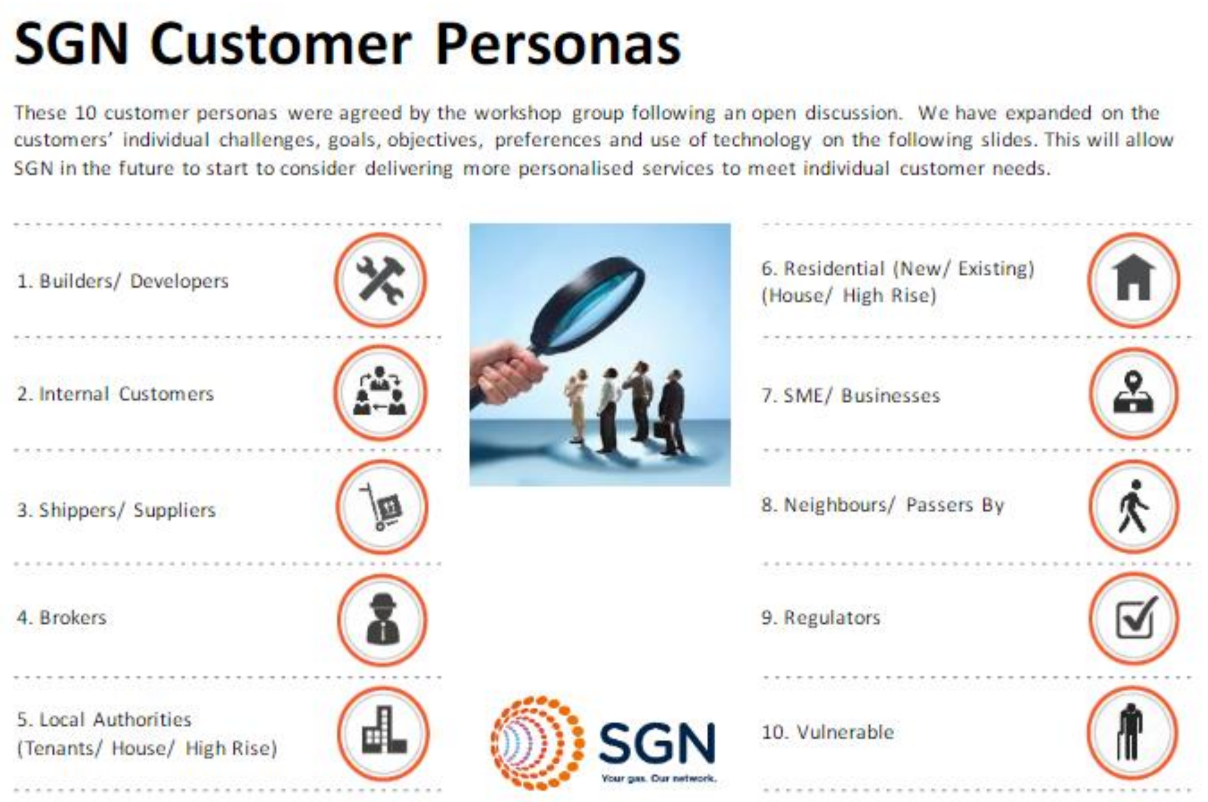
Conn	GSOS	Maintain or improve connections standards of performance and, voluntarily, extend standards to distributed gas connections.	IT availability standards for critical systems (99.5%), device replacement within 1 working day, incident response SLAs e.g. P1 incident response within 4 hours for critical systems, cyber incident response SLAs, vulnerability and patch management policy, architectural principles and security standards.	Front Office service provision (Maximo Work and Asset Management, ESRI Geospatial Asset Management, Click/Field Service Edge Scheduling, Agentry Work Management and Data Capture, Geofield Geospatial Data Capture, Digital Asset Maps, Insight Streetworks Management, Clearman Reinstatement Management), Back Office service provision (Oracle EBS, CIPS Contractor payment system), Cognos and Tableau reporting service provision, O365 and productivity service provision, system and infrastructure upgrades, support and maintenance.	BAU Capex, Front Office Replacement or Redesign, Network and Communications Refresh, Device Refresh, Data Governance and Quality, Regulatory and Mandatory Change, Cyber Security Investment, Integration Replacement, Back Office Replacement or Redesign

Customer	Broad Customer Measure	Satisfaction: maximise customer satisfaction score across three categories	IT availability standards for critical systems (99.5%), device replacement within 1 working day, incident response SLAs e.g. P1 incident response within 4 hours, for critical systems, cyber incident response SLAs, vulnerability and patch management policy, architectural principles and security standards.	Brochure Website (SGN) service provision, ReciteMe (translation and read aloud technology on the website) service provision, eCommerce Website (connections) service provision, CiTNow (Connections work outcomes video technology) service provision, eGain (CRM, Livechat, Social Media Monitoring, 2 way SMS) service provision, Connection Plan Dates (Connection appointment booking) service provision, Elgin Roadworks (online customer information portal) service provision, Stakeholder Relationship Management Database and Survey Tools service provision, Front Office service provision (Maximo Work and Asset Management), Back Office service provision (Oracle EBS) O365 and productivity service provision, system and infrastructure upgrades, support and maintenance.	Customer Experience and Stakeholder Investment in order to keep pace with expecations throughout GD2, BAU Capex, Front Office Replacement or Redesign, Network and Communications Refresh, Device Refresh, Data Governance and Quality, Regulatory and Mandatory Change, Cyber Security Investment, Integration Replacement, Back Office Replacement or Redesign, Future Technology Readiness (Data and Analytics)
		Complaints: minimise customer complaints across all 4 metrics			
		Engagement: identify key stakeholder issues, develop effective engagement and show change			

Environmental	Environ-mental (Broad measure)	Support the development of a low carbon energy sector through facilitating the connection of renewable gas sources as measured by the number of enquires and volume of capacity connected.	IT availability standards for critical systems (99.5%), device replacement within 1 working day, incident response SLAs e.g. P1 incident response within 4 hours for critical systems, cyber incident response SLAs, vulnerability and patch management policy, architectural principles and security standards.	SCADA and Telemetry High Pressure Network Control and Monitoring service provison, PMAC Pressure Management service provision, High Pressure Management Gas Quality Information System (HPMIS) service provision, Synergi Gas Low Pressure Modelling service provison, Falcon High Pressure Modelling service provision, O365 and productivity service provision, system and infrastructure upgrades, support and maintenance.	Telemetry Refresh, Control Room Replacement or Redesign, Non Core Application Refresh
	Gas transport losses	Manage and reduce the gas transportation network losses resulting from leakage, own use and theft from GD1 GWh baseline.		SCADA and Telemetry High Pressure Network Control and Monitoring service provison, PMAC Pressure Management service provision, High Pressure Management Gas Quality Information System (HPMIS), Theft of Gas Database service provision, O365 and productivity service provision, system and infrastructure upgrades, support and maintenance.	

3.3 Serving different customer groups

During GD1, we have targeted our customer and stakeholder investment across 10 specific and predefined customer groups. The attached table highlights the key areas where IT costs and investment in GD1 has been targeted across these groups.



SGN Customer Personas

These 10 customer personas were agreed by the workshop group following an open discussion. We have expanded on the customers' individual challenges, goals, objectives, preferences and use of technology on the following slides. This will allow SGN in the future to start to consider delivering more personalised services to meet individual customer needs.

1. Builders/ Developers
2. Internal Customers
3. Shippers/ Suppliers
4. Brokers
5. Local Authorities (Tenants/ House/ High Rise)
6. Residential (New/ Existing) (House/ High Rise)
7. SME/ Businesses
8. Neighbours/ Passers By
9. Regulators
10. Vulnerable

Customer personas	Associated IT services and investments
Builders/developers	New connections systems and new SGN website Asset mapping self-service (plant protection)
Internal customers	SharePoint, Office 365, End user compute services, IT service desk and My IT Hub/Service now Digital Hub (intranet) Yammer and Microsoft Teams and Skype Digital e-Timesheets Oracle Finance/HR and payroll Geofield – (geospatial mobile map viewer and asset update system) Cornerstone performance and learning management system
Shippers and suppliers' brokers	Xoserve and UK Link replacement (GDN funding in excess of £120m)
Local authorities (tenants, house, high-rise)	Insight system (Local Authority notification and works portal), riser database Elgin Roadworks (one.network): A joint website showing all Local Authority and utility roadworks with corresponding details for customers

Residential (new existing/house/high-rise	New website and redesign Reciteme: A translation and read aloud website Our e-commerce website redesign 10/10 app: our customer satisfaction survey and feedback tool Citnow: video messaging for new connections and alterations Connection plan dates and new connections systems e-gain customer engagement management solution managing live chat, two-way SMS, customer relationship management and social media interaction e.g. Facebook, Twitter etc
SME business	New connections systems and new SGN website Asset Mapping self-service (plant protection)
Neighbours/passers by	Elgin roadworks (one.network): A joint website showing all local authority and utility roadworks with corresponding details for customers 0800 111 999 emergency gas escape service Critical emergence response systems availability
Regulators	Implementation of regulatory change such as GDPR, UNC mods, Cyber Assessment Framework etc
Vulnerable customers	Priority Service Register and 10/10 customer satisfaction (specifically inked to identifying and capturing vulnerable customer details)
All of the above	Stakeholder relationship management software

We will apply the same rationale in GD2 to allocating IT investment expenditure by customer groups, in particular, vulnerable and hard-to-reach. In GD2, we will also continue to invest in our stakeholder relationship management software which will help us gain continued and improved insight and ensure high quality engagement to demonstrate our social and community role, and its responsibilities to future customers and stakeholders.

4 GD2 stakeholder insight

We have undertaken an extensive programme of engagement and research with customers and stakeholders in developing our business plan. Further information is provided in chapter 4 of our business plan and the Enhanced Engagement appendix.

4.1 Customer Engagement Group (CEG)

Our IT and Cyber resilience plan and approach has been shared with our CEG and we have taken the specific feedback from the group. The main feedback confirmed our plan aligned with key stakeholder expectations with regards to keeping the gas flowing safely and providing excellent service.

In addition, our CEG has stated its expectation we will provide independent validation and expert advice of their IT investment and run plans in order to ensure the proposed investment is in the correct areas and the value we are expecting to receive and spend is in-line with industry expert and analyst predictions.

The IT business plan has been validated by Gartner and the proposed spend is within their expected benchmark range. This report has been included as supporting evidence as part of our final business plan submission.

4.2 Stakeholder priorities

Our programme of customer research shows that customers view future energy solutions and keeping costs down as the priorities they would like us to focus on[3]. When specifically asked to rank attributes relating to the utilisation of technology and ease of access to information, customers indicated that these fell towards the lower end of the scale of importance to them[4]. However, customers rated designing the network to transport alternative greener gases as of comparatively high importance. Keeping the gas flowing and acting safely were also rated as high importance, for which our IT services are a fundamental component.

Similarly, our stakeholder satisfaction surveys[5] have revealed that utilising latest technology, whilst important, was less of a priority, relative to other considerations stakeholders felt we should prioritise. Other priorities, which are impacted by our IT investments, are however seen as a higher priority, such as reliability of gas supplies and providing good customer service[6].

4.3 Positive impact

Our research with customers and stakeholders has shown that increasingly, expectations are that we should utilise latest technology to provide better information and service. Investment in IT systems and infrastructure is critical in helping us to meet this expectation.

Customer expectation and satisfaction

Our proposed expenditure in GD2 is devoted to maintaining current customer satisfaction levels and keeping pace with increasing customer demands, in support of our 'Positive Impact' commitment. We know from our qualitative workshops our customers want us to keep pace with our current levels of customer service[7], and

[3] Stage 1: Explorative Qualitative Workshops and interviews (Exploratory Phase) (ref 002)

[4] Stage 2: Max Diff Prioritisation Phase Report (ref 003)

[5] SGN Stakeholder Satisfaction Wave 1,2 (teledepths) & 3 (data only) (ref 071,072,073)

[6] MFT Workshop March 2017 London, Portsmouth & Edinburgh (Ref 008,009,010)

[7] Shaping the Business Plan Qualitative workshops - Customer Service & Supporting Vulnerable (ref 085)

that it is a medium priority for further investment.

Due to this customer and stakeholder feedback, we have assigned the same costs for customer service investment as in GD1 (£0.5m p.a.). This will enable us to keep our current levels of customer satisfaction and keep pace with customer demands. Our independent assessment of this investment level by Gartner[8] indicated this was below the lower estimate expected by them in this area of technology spend.

The flexible and dynamic nature of customer expectations over the next five-year price control period means we will be required to explore multiple digital solutions to keep pace and be flexible in our approach. As is discussed in our business plan, there are multiple areas we will explore in GD2. Further details can be found in our customer and vulnerability plan appendix (023).

4.4 Delivering a safe and efficient network: safety, resilience and cyber security

Our safety critical and business operations are underpinned by highly available and secure IT systems. We therefore need to ensure our critical systems are secure and resilient to prevent interruption or disruption to our day-to-day business. In order to inform our IT security plans and strategy we have undertaken an ongoing and extensive stakeholder engagement process to ensure we are appropriately informed in our decision making and making the most educated decision given the uncertainty. Important points of reference include:

- **The cyber threat to critical national infrastructure (CNI) – UK Government risk assessment.**[9] UK Government identifies 'cyber' as one of six Tier 1 threats to national security. This note focuses on the cyber threat to the UK's critical national infrastructure, describes measures to improve cyber security and challenges in how to implement them. Such systems are increasingly connected into large networks to allow centralised monitoring and remote or automated control, to make operation and maintenance more efficient. These networks often connect to the internet, either directly or indirectly via the operators' other networks. As more industrial control systems connect to computer networks, the potential for cyber-attacks to cause physical effects increases. Computer-based CNI systems are vulnerable to electronic failure, design flaws, operator error, physical damage and cyber-attack.
- **Advanced persistent threat (APT) activity exploiting managed service providers.**[10] The National Cybersecurity and Communications Integration Center (NCCIC) is aware of ongoing APT actor activity attempting to infiltrate the networks of global managed service providers (MSPs). Since May 2016, APT actors have used various tactics, techniques, and procedures (TTPs) for the purposes of cyber espionage and intellectual property theft. APT actors have targeted victims in several U.S. critical infrastructure sectors, including Information Technology (IT), Energy, Healthcare and Public Health, Communications, and Critical Manufacturing.
- **Advisory: Russian state-sponsored cyber actors targeting network infrastructure devices.**[11] This advice provides information on the worldwide cyber exploitation of network infrastructure devices (e.g. routers, switches, firewalls, Network-based Intrusion Detection System (NIDS) devices) by Russian state-sponsored cyber actors.
- **Indicators of compromise for Malware used by APT28.**[12] Advanced Persistent Threat group, APT28 (also

[8] Gartner IT Cost and Capital Investment Assessment Project Report v1.2 15 March 2019

[9] http://researchbriefings.files.parliament.uk/documents/POST-PN-0554/POST-PN-0554.pdf

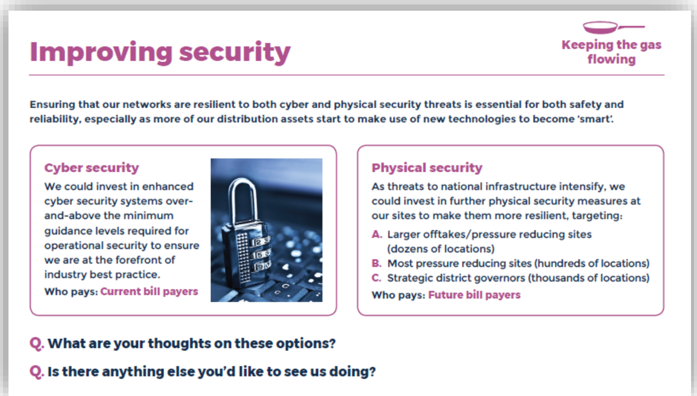
[10] https://www.us-cert.gov/ncas/alerts/TA18-276B

[11] https://www.ncsc.gov.uk/alerts/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices

[12]https://www.ncsc.gov.uk/content/files/protected_files/article_files/Indicators%20of%20Compromise%20for%20Malware%20used%20by%20APT28%20v.4.pdf

known as Fancy Bear, Pawn Storm, the Sednit Gang and Sofacy), is a highly skilled threat actor, best known for its disruptive cyber activity against the US Democratic National Committee (DNC).

- **Moving Forward Together stakeholder events[13].** At our workshops in March 2017, during a discussion relating to whether we were focussing on the right areas, our stakeholders stated it was important to be more explicit on cyber issues. At our workshops in March and November 2018 we considered the impact of technical change and investment to improve cyber security and resilience in more detail. Stakeholders suggested that it was important to listen to, and be guided by, the views of experts in this field. If attacks are already being experienced then the importance of this investment increases, and the consequences of a successful attack could be quite severe. It was suggested that adoption of a minimum standard, ideally backed by Government/Ofgem, or other expert bodies would be a sensible way to establish an appropriate level of resilience.



Improving security

Keeping the gas flowing

Ensuring that our networks are resilient to both cyber and physical security threats is essential for both safety and reliability, especially as more of our distribution assets start to make use of new technologies to become 'smart'.

Cyber security

We could invest in enhanced cyber security systems over-and-above the minimum guidance levels required for operational security to ensure we are at the forefront of industry best practice.

Who pays: Current bill payers

Physical security

As threats to national infrastructure intensify, we could invest in further physical security measures at our sites to make them more resilient, targeting:

A. Larger offtakes/pressure reducing sites (dozens of locations)
B. Most pressure reducing sites (hundreds of locations)
C. Strategic district governors (thousands of locations)

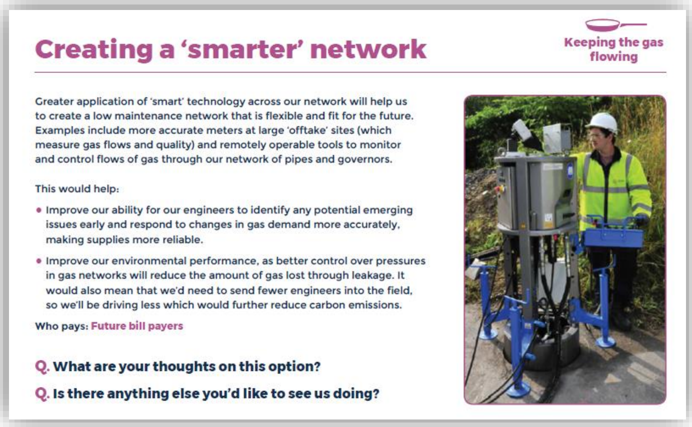
Who pays: Future bill payers

Q. What are your thoughts on these options?

Q. Is there anything else you'd like to see us doing?

  We have subsequently shared our plans and detailed approach with Ofgem to ensure this is in-line with its thinking. In response to this engagement and guidance, we have split our Cyber Security Investment plans between Business IT Security (IT) and Cyber Resilience (OT). We have provided full and complete costs of both but will provide more detailed plans on the latter as part of our ongoing engagement with Ofgem's Cyber Resilience team.

  Our stakeholders are generally of the view it is sensible to be taking steps to keep abreast of technological developments, and as these technologies advance, the associated costs should come down. It was identified by stakeholders as the energy system evolves in an effort to decarbonise, the application of smart technology will become increasingly important.



Creating a 'smarter' network

Keeping the gas flowing

Greater application of 'smart' technology across our network will help us to create a low maintenance network that is flexible and fit for the future. Examples include more accurate meters at large 'offtake' sites (which measure gas flows and quality) and remotely operable tools to monitor and control flows of gas through our network of pipes and governors.

This would help:

- Improve our ability for our engineers to identify any potential emerging issues early and respond to changes in gas demand more accurately, making supplies more reliable.
- Improve our environmental performance, as better control over pressures in gas networks will reduce the amount of gas lost through leakage. It would also mean that we'd need to send fewer engineers into the field, so we'll be driving less which would further reduce carbon emissions.

Who pays: Future bill payers

Q. What are your thoughts on this option?

Q. Is there anything else you'd like to see us doing?

- **Customer willingness to pay and acceptability testing.** Our first wave of willingness to pay research has included exploring customers willingness for investment in enhanced security to increase resilience to cyber threats. 76% of customers would support paying up to 46p on their gas bill for enhanced security to prevent cyber-attacks, with only 8% strongly opposed the idea.

  In addition, customers were asked a question in relation to enhancing our cyber security systems in our quantitative acceptability testing. This additional element of our plan attracted fairly high levels of acceptability from domestic customers in both Scotland and southern, at 75% in southern and 80% in Scotland. SME business customers tended to score this element the same or slightly higher than domestic

[13] MFT Workshops 2016,2017,2018 southern & Scotland (ref 006,007,008,009,010,011,012,013,014)

customers (79% for SME business customers in Southern and 80% for SMEs in Scotland).[14]

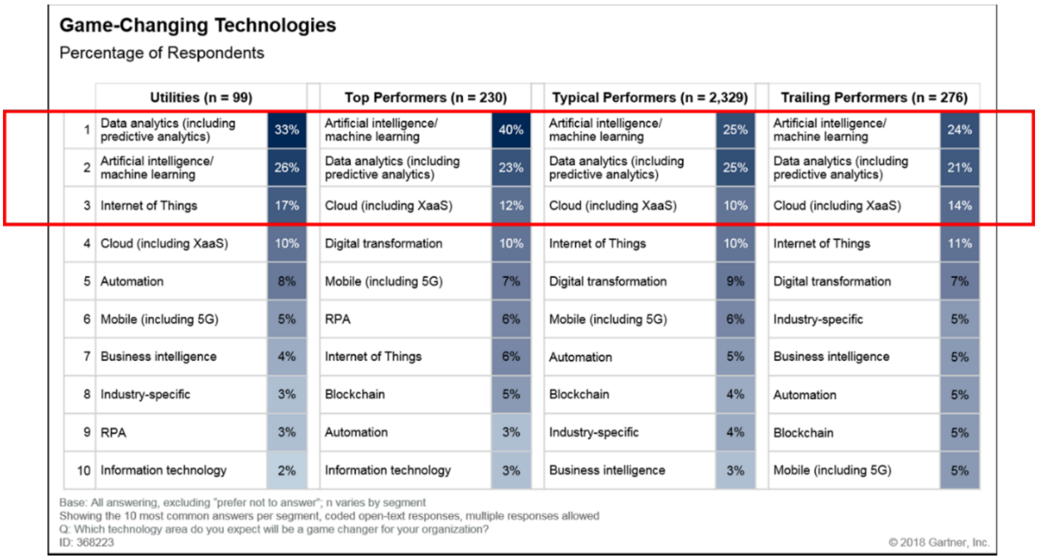
4.5 Shared future

As noted above, our programme of customer research has identified Future Energy Solutions as a priority area for future investment. Our stakeholders have also told us this is an area they expect us to treat as a high priority. We therefore need to ensure we have the technological capability to play a role in the decarbonised energy system of the future.

We have received multiple sources of advice and guidance to support the principle of future technology readiness and the technologies that are likely to be impacting our business in a significant way during GD2 (see supporting Engineer Justification Framework papers; Future Technology Readiness IIoT and Future technology Readiness Analytics and Artificial Intelligence and Open Data for more detail and extensive supporting evidence).

The table and report reference shown below from industry experts and advisors, highlights the game changing technologies requiring investment that affect the Utilities sector.

Figure 3: Game change technologies by sector, Gartner 2019[15]



Game-Changing Technologies

Percentage of Respondents

	Utilities (n = 99)		Top Performers (n = 230)		Typical Performers (n = 2,329)		Trailing Performers (n = 276)	
1	Data analytics (including predictive analytics)	33%	Artificial intelligence/ machine learning	40%	Artificial intelligence/ machine learning	25%	Artificial intelligence/ machine learning	24%
2	Artificial intelligence/ machine learning	26%	Data analytics (including predictive analytics)	23%	Data analytics (including predictive analytics)	25%	Data analytics (including predictive analytics)	21%
3	Internet of Things	17%	Cloud (including XaaS)	12%	Cloud (including XaaS)	10%	Cloud (including XaaS)	14%
4	Cloud (including XaaS)	10%	Digital transformation	10%	Internet of Things	10%	Internet of Things	11%
5	Automation	8%	Mobile (including 5G)	7%	Digital transformation	9%	Digital transformation	7%
6	Mobile (including 5G)	5%	RPA	6%	Mobile (including 5G)	6%	Industry-specific	5%
7	Business intelligence	4%	Internet of Things	6%	Automation	5%	Business intelligence	5%
8	Industry-specific	3%	Blockchain	5%	Blockchain	4%	Automation	5%
9	RPA	3%	Automation	3%	Industry-specific	4%	Blockchain	5%
10	Information technology	2%	Information technology	3%	Business intelligence	3%	Mobile (including 5G)	5%

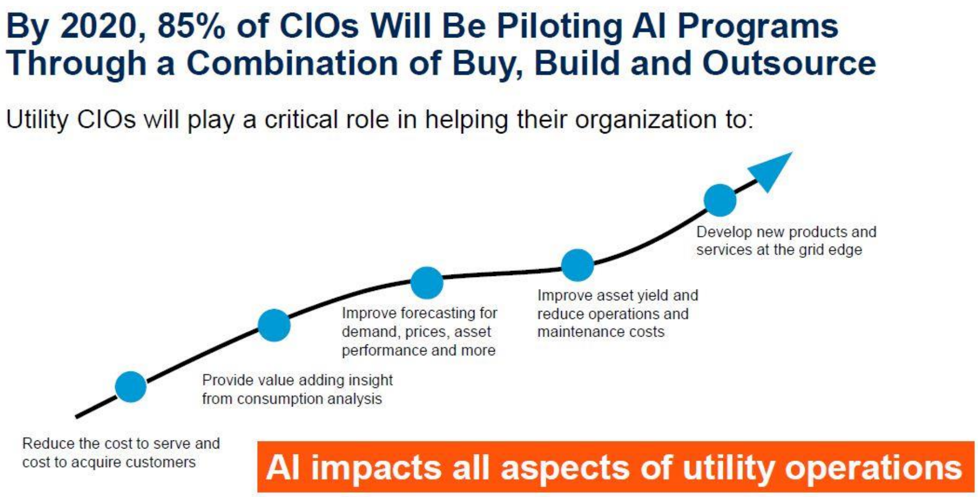
Base: All answering, excluding "prefer not to answer"; n varies by segment
Showing the 10 most common answers per segment, coded open-text responses, multiple responses allowed
Q: Which technology area do you expect will be a game changer for your organization?
ID: 368223

© 2018 Gartner, Inc.

[14] Business Plan Acceptability Testing Phase 2 (Ref 079)

[15] Gartner: 2019 CIO Agenda: Utility Industry Insights, Published: 15 October 2018 Gartner ID: G00368223

Figure 4: AI for business value, Gartner 2018[16]



By 2020, 85% of CIOs Will Be Piloting AI Programs Through a Combination of Buy, Build and Outsource

Utility CIOs will play a critical role in helping their organization to:

Reduce the cost to serve and cost to acquire customers
Provide value adding insight from consumption analysis
Improve forecasting for demand, prices, asset performance and more
Improve asset yield and reduce operations and maintenance costs
Develop new products and services at the grid edge

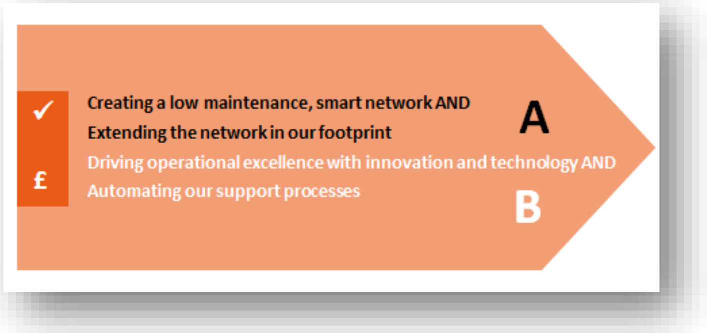
AI impacts all aspects of utility operations

Over and above the independent advice of Gartner, we have sourced multiple highly-respected technology advisors and partners and the following references further evidence of the need to prepare our company and its operations for the significant technology changes that will occur between now and 2026, these include:

- Artificial Intelligence: The Next Digital Frontier (McKinsey & Company, June 2017);
- Age of Analytics: (McKinsey Global Institute December 2016);
- Review of latest developments in the Internet of Things. (Cambridge Consultants - Tim Winchcomb, Sam Massey, Paul Beastall. March 2017);
- Harvey Nash/KPMG CIO Survey 2018;
- MIT technology Review – Engines of Insight 2018;
- Gartner 2019 CIO Agenda: Utility Industry Insights Published: 15 October 2018;
- Deloitte Consulting 2018 Global CIO Survey;
- Accenture and MIT (Massachusetts Institute of Technology) Winning with Analytics Report;
- Cap Gemini Transformation of intelligent utilities with analytics, big data; and
- ‘The Internet of Things (2017).

Investment in new technology

Stakeholders at our Moving Forward Together workshops in March 2018 participated in discussions on:

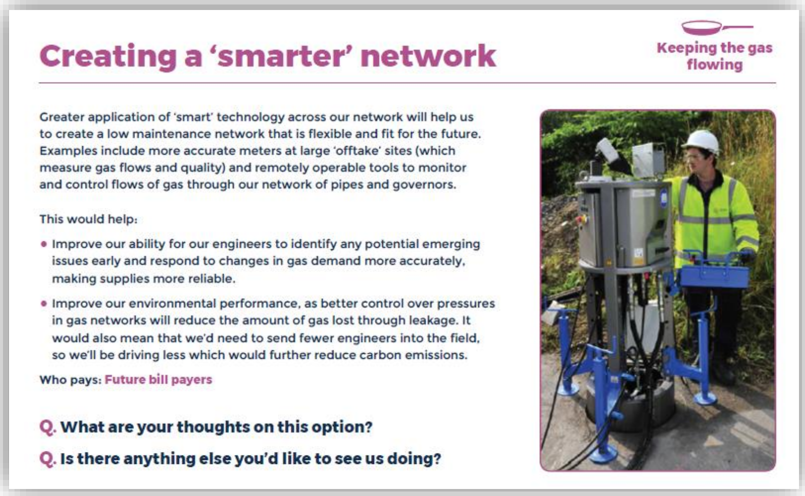


✓ Creating a low maintenance, smart network AND Extending the network in our footprint — A

£ Driving operational excellence with innovation and technology AND Automating our support processes — B

[16] Gartner: 2019 - AI for Business Value: Gartner Industry Presentation 04 Nov 2018

At our Moving Forward Together workshops in November 2018, we continued the conversation, with breakout groups discussing the following:



Creating a 'smarter' network

Keeping the gas flowing

Greater application of 'smart' technology across our network will help us to create a low maintenance network that is flexible and fit for the future. Examples include more accurate meters at large 'offtake' sites (which measure gas flows and quality) and remotely operable tools to monitor and control flows of gas through our network of pipes and governors.

This would help:

- Improve our ability for our engineers to identify any potential emerging issues early and respond to changes in gas demand more accurately, making supplies more reliable.
- Improve our environmental performance, as better control over pressures in gas networks will reduce the amount of gas lost through leakage. It would also mean that we'd need to send fewer engineers into the field, so we'll be driving less which would further reduce carbon emissions.

Who pays: Future bill payers

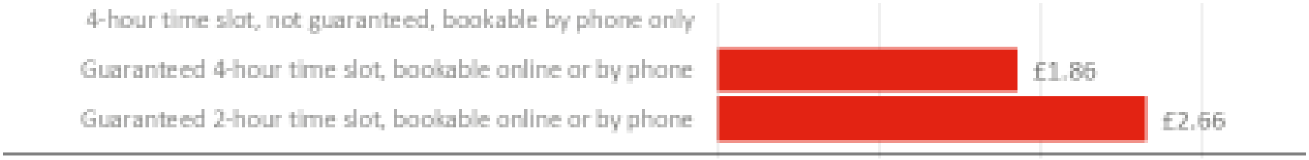
Q. What are your thoughts on this option?

Q. Is there anything else you'd like to see us doing?

Stakeholders were generally of the view it is sensible to be taking steps to keep abreast of technological developments, and that as these technologies advance, the associated costs should come down. It was identified by stakeholders that as the energy system evolves in an effort to decarbonise, the application of smart technology will become increasingly important and we have taken this on board in our proposed areas for investment.

4.6 Customer outage management

Our willingness to pay research with customers includes appetite for greater flexibility and guaranteed timings in relation to planned visits to their property. Results from domestic customers were as follows:



We worked in collaboration with the other gas networks to explore customer appetite for guaranteed appointment times. The combined research we did with the other GDNs demonstrated that less than 20% of people who had actually experienced an outage would have wanted a timed appointment for a purge and re-light. For this reason, we have not included costs associated with systems and IT changes associated with customer outage management.

5 Relevance to GD2 cross-sector issues

5.1 Innovation, decarbonisation and whole systems

The Energy Data Taskforce has developed five recommendations within their report: A Strategy for a Modern Digitalised Energy System (summarised here):

1. Digitalisation of the Energy System - Government and Ofgem should use existing legislative and regulatory measures to direct the sector to adopt the principle of Digitalisation of the Energy System in the customers' interest.
2. Maximising the value of data - Government and Ofgem should direct the sector to adopt the principle that Energy System Data should be 'presumed open', supported by requirements that data is 'discoverable, searchable, understandable', with common 'structures, interfaces and standards' and is 'secure and resilient'.
3. Visibility of Data - A Data Catalogue should be established to provide visibility through standardised metadata of Energy System Datasets across Government, the regulator and industry.
4. Coordination of Asset Registration - An Asset Registration Strategy should be established to increase registration compliance, improve the reliability of data and improve the efficiency of data collection.
5. Visibility of Infrastructure and Assets - A unified Digital System Map of the Energy System should be established to increase visibility of the Energy System infrastructure and assets, enable optimisation of investment and inform the creation of new markets.

Martin Cave, Ofgem chairman, said: *"Data will play a crucial role in enabling competition and innovation to drive down prices for customers and provide them with new products and services. This is why Ofgem fully supports the Taskforce's five recommendations to improve data use. We will be working with BEIS, consumer groups and the industry to ensure better use of data unlocks a brighter future for energy consumers."*

Chris Skidmore MP, Energy and Clean Growth Minister, said: *"Transparent and accessible data will become ever more important as the UK develops its smart, green energy system. The way we share and harness that data will help us all as we move towards the greater use of low carbon technologies such as solar panels, battery storage systems and electric vehicles. The recommendations in this report will help to ensure data is at the forefront of our low carbon energy system which will continue to go from strength to strength as we power towards becoming a net zero economy by 2050."*

The technology themes highlighted within our future technology readiness plans for GD2 and our proposals around open data provision have been heavily influenced by the recommendations and direction highlighted by the Energy Data Taskforce (see supporting Engineering Justification Framework papers for more detail). Additionally, these themes have been exploited and progressed by numerous innovation projects we have already undertaken where connected 'things' have been developed, utilised and either have been, or are in the process of being, rolled-out to our operational environment. These are examples of IIoT technology which in themselves generate and issue new and different data sources, never previously available to manage and operate our network.

In addition to ensuring sufficient funding for implementation of the technology supporting these areas, it is vital that continued research, development and low technology readiness innovation funding is provided to support the further progression of the recommendations made by the EDTF.

Examples of the projects that have been developed in GD1 are:

Project name	Reference	Project overview	Link to project detail
Network Innovation Allowance (NIA) projects			
Advanced gas detection	NIA_SGN0064	The objectives of the project are to produce a portable gas detection device to detect methane and CO gases and determine if readings detected on site are from a natural gas leak. These readings are then automatically linking to geospatial positions as a digital record of work	http://www.smarternetworks.org/project/nia_sgn0064
Remote pressure control and management	NIA_SGN0122	The project is delivering the ability to remotely adjust gas pressures via connected pressure management devices	http://www.smarternetworks.org/project/nia_sgn0122
Remote site monitoring	NIA_SGN0110	This project is developing probes which can be left at sites and will send automatic gas reading to the cloud for management of potential gas escapes	http://www.smarternetworks.org/project/nia_sgn0110
Automated pressure tester	NIA_SGN0079	This device aims to help ensure the accuracy and consistency of the testing of gas pressures and data recording process while removing the potential for human error and providing the opportunity to automatically update our asset records through a suitable cloud-based service	http://www.smarternetworks.org/project/nia_sgn0079
Osprey pressure validator	NIA_SGN0021	A wireless, intrinsically safe, battery-powered remote monitoring unit that fits inside bollards, posts and meter boxes and monitors gas pressure up to 100mbar	http://www.smarternetworks.org/project/nia_sgn0021
Network Innovation Competition (NIC) projects			
Robotics – CIRIS and CISBOT	SGNGN01	In addition to repairing, remediating and inspecting our pipes while significantly reducing customer disruption, these robots provide in pipe inspection video data as well as other data relating to potential corrosion and/or asset health	http://www.smarternetworks.org/project/sgngn01
Real Time Networks	SGNGN03	This project has resulted in essentially making part of our distribution network “smart” by applying weather, flow, gas quality and demand sensors across the Medway region of our distribution network. The additional application of these sensors provides SGN with significantly more data and information from which we can assess our forecasting and demand management models	http://www.smarternetworks.org/project/sgngn03

In addition to applying the technology changes demonstrated by these innovation projects, our IT department promotes and develops and innovation culture through working with partners, applying new ways or working such as lean and agile working practices, developing proof of concepts and working closely with innovative vendors who excel in innovation such as Amazon and Microsoft.

Although still a relatively immature technology, we also believe ‘blockchain’ is an opportunity for the UK energy industry, with the potential to play a significant role in future proofing networks and supporting energy transition.

UK industry on the whole, is still waking-up to its potential, although the UK Food Standards Agency is one example of where it is being applied as a regulatory tool to ensure compliance in the food sector. Ofgem’s focus on whole systems thinking and integration should provide the impetus and opportunity for collaboration to investigate blockchain and drive the development of the right applications in our regulated environment.

Because it’s new but with potential for longer term benefits, blockchain is a prime candidate for R&D as part of the innovation stimulus, particularly around new technologies which have a lower technology readiness within our industry.

We have provided a service enhancement opportunity for customers around the advancement and provision of Open data. This is primarily in response to the EDTF’s recommendations and associated guidance from Ofgem around digitalisation. We’ve provided a cost estimate associated with this capability as defined within he associated EJP and CBA. We estimate that the cost would be £3.5m as capital expenditure. This has been broadly supported by stakeholders who recognised the importance of technology as the energy system evolves to decarbonise.

We have further defined our digitalisation ambition within the associated Digitalisation strategy which is published on our website in line with Ofgem’s guidance.

In addition to the above, our continued investment in cloud based, low energy consumption data centres and mobile technology solutions that result in less travel and fleet emissions and our continued ethical disposal of IT equipment will further drive and support our Environmental Action Plan as laid out in the associated appendix (003).

5.2 Resilience

Cyber Security across our entire organisation is a fundamental point of resilience and the evidence of the need to support a substantial increase Cyber Security capability in order to ensure the ever-increasing threat of cyber-attack on UK Critical National Infrastructure (CNI), and UK Gas Networks in particular, is managed and adequately funded is wide and broad ranging.

This evidence comes from UK Government and Ofgem which is seeking a significant improvement and far reaching assessment of GDNs’ Cyber Security as part of the Network Information Systems Directive (NIS D). BEIS and NCSC are working actively with us, the other UK GDNS and Ofgem to ensure we are adequately funded through the regulated price control and that this funding is appropriately assessed and measured. This capability and associated resilience are required across our entire organisation and not just in relation to CNI assets. As an example, the resilience and availability of our gas escape emergency response is directly linked to our cyber security capability across our entire IT organisation. Failure to provide adequate security across such safety critical IT services, poses a material risk to life and property.

- **UK National Cyber Security Strategy 2016-2021[17].** The national cyber security strategy identifies that cyber-

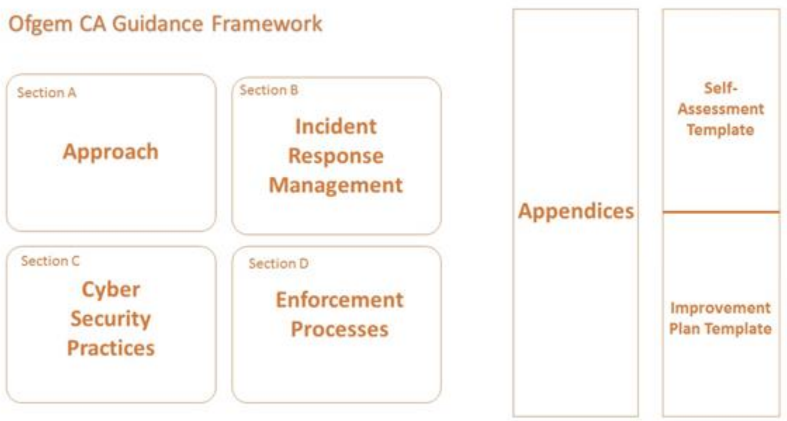
[17] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachmentdata/file/567242/national cyber security strategy 2016.pdf

attacks are growing more frequent, sophisticated and damaging when they succeed. As a result, it sets out plan to defend systems and infrastructure, deterring adversaries, and developing a whole society capability and announcing a new National Cyber Security Centre to provide a hub of expertise, as well as rapid response to major incidents.

- **Network and Information Systems Regulations 2018 NIS Regulations (NIS-D)[18].** Network and information systems and the essential services they support play a vital role ensuring the supply of energy. Their reliability and security are essential to everyday activities. In 2013 the EU put forward a proposal to improve the EU's preparedness for a cyber attack. This proposal became the directive on the security of Networks and Information Systems (the NIS Directive) in August 2016.

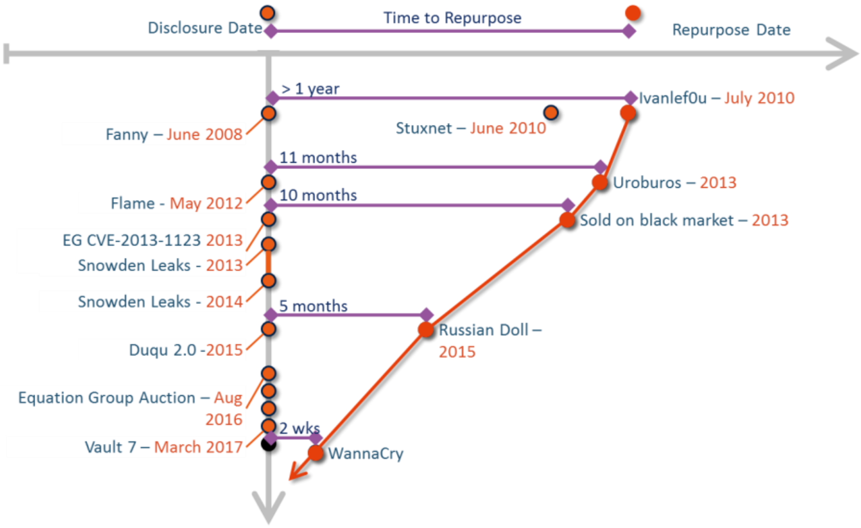
  As we have seen from numerous cyber security incidents these systems can be an attractive target for malicious actors, and they can also be susceptible to disruption through single points of failure. The magnitude, frequency and impact of network and information system security incidents is increasing. Events such as the 2017 WannaCry ransomware attack, the 2016 attacks on US water utilities, and the 2015 attack on Ukraine’s electricity network clearly highlight the impact that incidents can have.

  There is therefore a need to improve the security of network and information systems across the UK, with a particular focus on essential services which, if disrupted, could potentially cause significant damage to the economy, society and individuals’ welfare. We have been party to several meetings with Ofgem to define and agree this framework and highlighted the need for it to be linked to the GD2 price control mechanism.



  These requirements have been discussed in a number of stakeholder meetings with both Ofgem and BEIS, and the wider energy utilities sector via the Energy Emergencies Executive Committee (E3CC) group.

- **Risk advisories and threat response.** The threat response time all companies now face when aiming to deal with cyber threats has moved from c.12 months in 2012/13 (the beginning of GD1) to less than a fortnight as was the case with the WannaCry attack experienced in 2017.



  This compression of time to respond to malware and cyber-attacks means that companies risk a higher level of exposure and disruption to operations if they are unable to detect, protect and respond to these attacks in a

[18] https://www.ncsc.gov.uk/guidance/introduction-nis-directive

matter of hours and days rather than months. This means that those companies who are at high risk, such as CNI organisations like the GDNs, need to have a significantly improved Cyber security capability. The diagram above illustrates this compression of the time to response by citing real examples of attacks and malware that occurred:

- **Energy emergencies executive committee - Cyber security task group.** The Cyber Security Task Group of the Energy Emergencies Executive Committee (E3C) is formed from a group of the most significant UK critical national infrastructure operators of electricity and gas transmission and distribution, and electricity generation.

This amounts to 20 operating companies (increased to 24 to cover the scope of the Network Information Security Directive) together with invited participants from the cybersecurity policy unit of BEIS, the National Cyber Security Centre (NCSC) and associate membership from Ofgem and the BEIS NIS Directive regulatory team. This group provides reporting on the evidence and real examples of the level of industry engagement and workload required to adequately address and continually improve our Cyber Security. This looks across the supply chain, joint working skills development and sharing best practice.

- **Current - operational technology (OT).** More than in most other sectors, cybersecurity incidents in industrial environments can result in physical consequences that can cause threats to human lives as well as damage to equipment, infrastructure, and the environment. While there are certainly traditional IT-related security threats in industrial environments, it is the physical manifestations and impacts of the OT security incidents that continue to be a risk priority for us and other GDNs.

In addition to physical damage, operational interruptions have occurred in OT environments due to cybersecurity incidents. For example, in 2000, the sewage control system of Maroochy Shire in Queensland, Australia, was accessed remotely, and it released 800,000 litres of sewage into the surrounding waterways. In 2015, the control systems of the Ukrainian power distribution operator Kyiv Oblenergo were remotely accessed by attackers, causing an outage that lasted several hours and resulted in days of degraded service for thousands of customers.

- **Future - operational technology.** The risk from cyber security incidents in Gas Control environments and our wider operational environment that cause threats to human lives as well as damage to equipment, infrastructure and the environment is set to remain. Technical conversion between IT and OT environments are set to continue with more connected ‘things’ utilising cloud services over the internet.

This is true of our distribution network as much as our transmission network and therefore is not solely rated to CNI assets, thus creating a more complex and fragmented network that will require additional security coverage as evidenced in section 5.1.

- **Current - threats.** Historically, attackers were skilled individuals with deep knowledge of technology and the systems they were attacking. However, as technology has advanced, tools have been created to make attacks much easier to carry out. To further complicate matters, these tools have become more broadly available and more easily obtainable. Compounding this problem, many of the legacy protocols used in IoT environments are many decades old, and there was no thought of security when they were first developed. This means that attackers with limited or no technical capabilities now have the potential to launch cyber-attacks, greatly increasing the frequency of attacks and the overall threat to end operators. A new an increasing threat is the sophistication of nation state targeted attacks, either meant deliberately to effect operations or as staging posts for future disruption.

- **Future - threats.** Nation-state attacks described as Advanced Persistent Threats (APT’s) are predicated to continue. NCSC and the US cert issued several advisories during 2017/18 identifying APT’s attack patterns moving across the supply chain. The supply chain remains a prioritised risk for GDNs across their IT and OT estates.

- **Networks.** Communication networks, both local and geographically dispersed, have been used in industrial environments for decades. For example, remote monitoring of substations in utilities (e.g. pressure reduction sites and governors) and communications between semi-autonomous systems in manufacturing are long-standing examples of such OT networks. These OT-specific communication systems have typically been standalone and physically isolated from the traditional IT enterprise networks in the same companies. While it follows the traditional logic of 'security through obscurity', this form of network compartmentalisation has led to the independent evolution of IT and OT networks, with interconnections between the environments strictly segregated and monitored.

The isolation between industrial networks and the traditional IT business networks has been referred to as an 'air gap', suggesting there are no links between the two. While there are clearly examples of such extreme isolation in some industries, it is actually not an accurate description of most IoT networks today. Broadly speaking, there is a varying amount of interconnection between OT and IT network environments, and many interdependencies between the two influence the level of interconnection.

This evolution of ever-increasing IT technologies in the OT space comes with the benefits of increased accessibility and a larger base of skilled operators than with the nonstandard and proprietary communication methods in traditional industrial environments. The challenges associated with these well-known IT standards is that security vulnerabilities are more widely known, and abuse of those systems is often easier and occurs on a much larger scale. This accessibility and scale make security a major concern, particularly because many systems and devices in the operational domain were never envisioned to run on some shared, open standards–based infrastructure, and they were not designed and developed with high levels of built-in security capabilities.

Projects in industrial environments are often capital intensive, with an expected life span that can be measured in decades. Unlike in IT-based enterprises, OT deployed solutions commonly have no reason to change as they are designed to meet specific (and often single-use) functions and have no requirements or incentives to be upgraded. A huge focus and priority in OT is system uptime and high availability, so changes are typically only made to fix faults or introduce new system capabilities in support of that goal. As a result, deployed OT systems often have slower development and upgrade cycles and can quickly become out of sync with traditional IT network environments. The outcome is that both OT technologies and the knowledge of those looking after those operational systems have progressed at a slower pace than their IT counterparts.

Most of the industrial control systems deployed today, their components and the limited associated security elements were designed when adherence to published and open standards were rare. The proprietary nature of these systems meant threats from the outside world were unlikely to occur and were rarely addressed. There has, however, been a growing trend whereby OT system vulnerabilities have been exposed and reported.

5.3 Business IT security and cyber resilience plans

We operate a centralised IT & cyber security operations model. This has proven to be the most cost effective and efficient support model to ensure adequate service support. While we have invested heavily in cyber security to ensure coverage of OT cyber risks such as dedicated monitoring of SCADA systems, asset management of the OT environment and cyber risk monitoring. Security logging, incident alerting and incident management remain a centralised service managed via our managed security service provider. In addition, platform services like End User Computing device encryption, virus scanning, network security monitoring and firewall management costs sit under the IT cost but underpin our ability to provide these services across our OT estate and assets. This approach ensures we maintain consistent continuity of security monitoring and response operations. A cyber security breach on an IT system can be as detrimental to customer outcomes as a breach on the OT system, as was demonstrated by the WannaCry virus in 2017.

However, in-line with the guidance we have revived from Ofgem as part of our GD2 plan review and consultation, we have attempted to delineate and separate Business IT security costs and Cyber Resilience costs. We highlight this has resulted in a false allocation and delineation of services and costs that are centralised and shared. Privileged Access Management as an example, is a centralised solution, cost and capability that sits across our entire estate. We have however derived a percentage of these costs to managing our OT estate. It is very important to note however, these costs are not incurred in this separate and delineated nature. It is also very important to bear in mind that the interconnected nature of IT and OT, means at a technical and physical level, the cyber risks facing both are also shared. E.g. external attacks on vulnerabilities in desktop or laptop operating systems can be used to exploit our control room and other OT services.

Compromise of our Active Directory, for example which is seen and defined by Ofgem definitions as Business IT Security, could result in escalation of privileges that exploit and compromise the OT and therefore, affect Cyber Resilience. For this reason, in addition to the defined and dedicated OT security investment projects, we have allocated a notional percentage of shared Security service costs to OT based ‘Cyber Resilience’ as requested. However, we believe it is imperative our Business IT Security Plan and Cyber Resilience plans are looked at jointly due to the reasons outlined above. We understand from recent meetings with Ofgem this is in-line with Ofgem’s thinking and separate funding for OT based Cyber resilience is likely to be treated under use-it-or-lose-it arrangements and as a likely reopener.

5.4 Cyber resilience: Appropriate and proportionate measures

The proportionality and appropriateness of measures have been captured within the parameters defined by Ofgem as part of the NIS-Directive and documented within our Cyber Assessment Framework (CAF).

- Sections 2.6 ‘proposed improvements’ was developed by following Ofgem guidance to determine proportional measures;
- Section 2.7 ‘mitigation priorities’ was developed following Ofgem guidance to ensure appropriateness was captured in reference to our cyber risk register; and
- Organisational changes required to support future OT management is captured within our CAF return.

To deliver the Ofgem NIS-D requirements in addition to managing our ever-increasing Cyber Risk profile across our entire IT estate, we have proposed doubling the size of the security team over the course of the next five years to supplement all five domains of Identify, Protect, Detect, Respond, Recover.

Compliance and risk identification have been captured within the parameters defined by Ofgem as part of the NIS-Directive and documented within our CAF.

- Section 2.2 ‘compliance and risk identification’ were developed by following Ofgem guidance to determine compliance measures;
- Section 2.3 ‘risk assessments’ were developed by following Ofgem guidance to determine risk identification based on sources of threat intelligence identified via several sources including but not limited to our membership of the E3CC (utility cyber security group) a collaboration group attended by NCSC and BEIS. We receive regularly threat advisory notices from NCSC, either specific to wider industry, sector or on rare occasions specific to us. Additionally, we receive threat notifications from several other sources including Symantec the largest and leading security company in the world. Additionally, Fujitsu our managed security provider has a threat intelligence service where again we are notified of threats to our sector. We also receive threat feeds from our vendor security community such as Schneider electric.

We have identified in detail, the specific initiatives to improve our cyber risk management capability. This is fully defined and explained within the supporting Engineering Justification Paper and associated Cost Benefit Analysis (CBA). We have directly linked our management of threats and cyber risk to the Cyber Assessment Framework and associated categories. It is important to note this is the investment based on today’s requirements and understanding and will change during GD2 as new threats emerge. It is also important to note these requirements do not reflect any new or emerging requirements from Ofgem such as the October 2019 guidance and consultation which is yet to conclude and any subsequent changes. We will continually assess and confirm the right areas of investment by utilising the CAF assessment and associated findings, interaction and advice from industry and advisor bodies such as the E3CC group, cyber security advisors, vendors and continued interaction and collaboration with Ofgem's Cyber resilience team.

In addition to the above, we will continue to use internal Key Performance Indicators (KPIs) to continually assess and ensure investment in Cyber Security is appropriately targeted and effective. The attached list of KPIs is a sample of the types we use as Cyber Security measures.

Operational security metrics:

- Patch coverage and latency e.g. number of critical patches applied within a period;
- Antivirus coverage e.g. percentage coverage of Antivirus across the estate.

Security incident management:

- Total number of security incidents reported monthly;
- Total number of incidents addressed within agreed timescales.

Compliance:

- Percentage of total number of critical systems or processes audited;
- Number of very high, or high-risk issues as an outcome of audits.

Access control:

- Number of privileged access accounts that have been inactive for a set number of days;
- Number of accounts that have not been disabled for leavers.

External threat level

- Global security threat levels;
- UK utilities threat level.

The metrics stated above are a subset of current operational reports in line with current governance structure and is not an exhaustive list.

A detailed list of the areas we intend to invest in throughout GD2 is defined within the accompanying Engineering Justification paper: Cyber Security. It is important to note that although we have undertaken extensive analysis and cost estimation to derive these plans, the nature of Cyber Risk is that it is ever changing and will require a degree of flexibility in where and how Cyber Security investment is targeted.

We will continually assess and confirm the right areas of investment by utilising the CAF assessment and associated findings, the KPIs listed above, interaction and advice from industry and advisory bodies such as the E3CC group, Cyber security advisors, vendors and continued interaction and collaboration with Ofgem's Cyber Resilience team.

6 GD2 activity breakdown

For clarity and visibility, we have defined our future plan in terms of ‘Run’ and ‘Investment’. This splits the investment plan into six key areas:

- **IT run costs** - This is expenditure required to keep daily service operations running and delivering existing IT service standards;
- **Mandatory IT investment** - IT Asset health investments. This is the investment required to ‘keep the lights on’ and ‘the gas flowing’ including responding to legal and Regulatory change;
- **Customer driven investment** - Maintaining existing levels of customer service while keeping pace with increasing expectations of customers;
- **Cyber security investment** - Investment relating solely to tackling the ever-increasing cyber risk;
- **Investment in future technology readiness** - Investment in GD2 on technologies that are demonstrated by research and technology advisors to be highly impactful on our industry and how we operate; and
- **Additional outputs** - Stakeholder led additional requirements and outputs. In particular, providing Open data capability and utilising smart meter data via DCC membership.

6.1 IT run costs

IT ‘Run’ costs relate to the predominantly operational expenditure required to keep our day-to-day services running. These services enable our business to operate safely, reliably and efficiently.

Failure to perform these services effectively would result in our inability to run our core operational services leading to major IT service failure and operational impact. This would result in us failing some or all of our licence, HSE and statutory obligations.

The Gartner assessment[19] demonstrates the existing IT services being run by us are proven to be run extremely efficiently and below average costs when compared to industry peers. The ongoing run costs of these services moving into GD2 equates to an average operational cost of £28.4m a year.

When taking into account the additional run costs associated with new services, in which to invest and deliver during GD2, and which includes ‘mandatory IT investment’, ‘Mandatory Business Driven Investment’, ‘Cyber Security Investment’ and ‘Future Technology Readiness’, the total ongoing average run costs for our IT investment equates to £32.3.m a year.

Due to the nature of our business, our IT investment is required to provide safety critical, highly responsive and available services and to ensure these are secure and addressing cyber security risk.

To give a sense of scale, our IT estate runs, maintains and supports:

- 5,200 end user devices and an annual volume of over 70,000 service desk contacts;
- We run and maintain over 650 TB of storage and 1,300 servers (900 windows and 400 Unix servers);
- We connect and support 47 separate physical site locations and over 14,000 Local Area Network Ports;
- In 2018, we received and monitored over 47 billion security logs. Every month we collect and monitor on average over four billion security logs and investigate on average 100 potential security incidents every month; and
- We receive on average, over 700,000 emails each month and stop over 100,000 spam and/or malware e-mail coming into the organisation each month.

[19] Gartner report – being provided with our business plan submission

In addition to the above, we also must manage CNI level security across our OT and control room environment which maintains and manages our gas network. This covers:

- Monitoring of over 3,000 km of pipeline;
- Over 11,000 telemetered data points updated every 60 seconds;
- 600 telemetered outputs (controls);
- 3,000 calculated data items automatically executed in the system;
- 400 DNCS alarms sound a day on average;
- 155 sites connected by satellite to two ground stations both located in the UK;
- Approximately 170 sites connected by UHF Radio system;
- The secure management of seven years of historic real-time data; and
- Secure collection and of roughly 1.7 GB of data every week

A summary of our GD1 run costs compared to GD2 run costs are shown below (in £000s):

Table 2: IT run costs

SGN (£m)	13/14	14/15	15/16	16/17	17/18	18/19	19/20	20/21	21/22	22/23	23/24	24/25	25/26
Employees	3.55	4.30	5.65	5.96	6.03	6.36	4.46	6.30	6.56	6.56	6.56	6.56	6.56
Ongoing costs	17.61	18.32	18.44	17.14	20.18	28.54	25.81	20.15	23.02	25.03	26.36	27.62	28.96
Total IT run	**21.16**	**22.62**	**24.09**	**23.10**	**26.21**	**34.91**	**30.28**	**26.45**	**29.57**	**31.59**	**32.92**	**34.18**	**35.52**

Please note this table shows run costs only and not total opex

6.2 Ongoing efficiency and cost drivers:

IT costs are made up of employees, hardware, software and third party services. We have taken our GD1 2018/19 costs as the baseline for our ongoing GD2 run costs. The Gartner benchmarking assessment demonstrates these existing IT services we run, are proven to be extremely efficiently and below average costs when compared to industry peers. We will also ensure GD2 investment costs are efficient. In order to ensure value for money during the GD2 period, every proposed project will be assessed and the most appropriate methodology selected to ensure the most cost-effective delivery solution and the prevention of stranded or underutilised IT assets and services.

We follow a PRINCE2-based quality gate approach to projects, ensuring rigour around governance, financial tracking and benefits realisation. At each stage gate as well as project artefacts being reviewed and checked, the business case will be revisited to ensure it still stands up. Solutions will be built in line with our IT Strategy while ensuring architectural principles and security standards are adhered to unless a clear exemption is provided. Our IT Strategy outlines a Cloud-first, buy, not build approach, ensuring the total cost of ownership of all solutions is the most appropriate for the size and scale of change. We are required under EU procurement law to market test every investment and external expenditure above £325,000. This ensures a transparent and open process as well as ensuring we select the most cost-efficient solutions and services available on the market.

Our investment cost options have been assessed and detailed in the accompanying Engineering Justification Papers and cost benefit analysis information. Each area of investment has been independently assessed and assured by Gartner as demonstrated in our supplementary benchmarking and assurance report.

6.3 Mandatory IT investment

Projects that sit within this category fall under the profile of presenting an unacceptable risk to our ability to operate if not undertaken. This includes functions such as our ability to respond to Gas Escape emergencies, pay our staff and suppliers and /or meet our legal, statutory, licence conditions and deliver against HSE requirements.

If we were not to continue to invest in the maintenance and upkeep of these services, we would not be able to meet our licenced obligations nor our legal or statuary company obligations.

In order to manage and maintain the IT estate, investment will be required in these areas to ensure continuity of service throughout the GD2 period. Investment will cover keeping the application estate up-to-date, ensuring devices are able to run and access applications and meet changing business and customer needs and ensuring CNI site monitoring and gas and network control is managed and maintained as required to meet both current and future requirements.

Broadly, mandatory IT investment can be categorised into the following technology platforms and cost categories which underpin our business. Each area has been defined and justified within individual Engineering Justification Papers and Cost Benefit Analysis where the current systems, options considered, timing and detailed cost breakdown are provided:

Investment area	Description
Application management	This is the activity to refresh upgrade and where end of life, replace all of business applications that are not considered front or back office e.g. Engineering applications such as DNV GL systems, and operational work management systems such as Insight, Clearman, Kony and Geofield
Front office systems	Replacement or refresh of safety critical front office applications. These systems support our emergency response and core operational services i.e. Maximo, Agentry/Syclo and Clickschedule. Safe and Reliable Network scenario assumes like-for-like upgrades and where end of life, replacement
Back office systems	Back Office systems enable us to pay employees and suppliers and run finance, HR and procurement services which are essential to our operation. Our Oracle roadmap and wider finance, HR and procurement systems will require a like-for-like upgrade/refresh, or where end of life, replacement during GD2
Network and communications	The voice and IT connectivity required for our workforce and locations to access our core systems. In GD2, a replacement and refresh of network and communication assets is required to ensure continuity of service
Application integration	Our IT estate needs to interface and interact with other systems internally and externally. E.g. Emergency response interfaces and Xoserve interfaces. Our integration platform will require upgrade and refresh during GD2 including the creation of new APIs to enable re use and new business capabilities

Financial planning and reporting	Replacement of financial planning and reporting tools
Telemetry	Refresh of physical telemetry communication technology required for our CNI sites. Failure to do so will inability to adequately monitor these sites
Device refresh	Replacement and refresh of end user devices to ensure continuity of service (laptops, desktops, tablets and phones)
BAU capex	Fix on fail, printers, peripherals, phones. GD2 sees a year on year increase associated with increased demand for devices as technology requirements change
Network control systems	Replacement and refresh of core control room services including SCADA and Network Monitoring and Modelling Applications. This covers essential refresh and replacement activity
Regulatory and legal change	This covers changes being driven by code and regulatory body changes such as faster switching, GDPR etc. The values have been derived based on known spend in GD1. Increased amount in year one and two reflects the likelihood of increased requirement for regulatory change as we enter into the GD2 period
Data governance and quality	Data Management Tooling required to support data governance assurance and maintain accuracy of statutory and regulatory reporting quality

Projects we have identified as mandatory are defined in detail within the accompanying Engineering Justification Papers and the associated impact on the business is defined if this investment is not made in each individual case. Phasing is based on asset life, asset/service health, end of support agreements, and historical spend profiles. In some cases, where technical solutions are yet to be fully defined, the capex and opex treatment is not fully detailed. However, we have taken current accounting policies and historical evidence in the last two years of GD1 to inform the capex/opex treatment of the investment.

Our mandatory IT investment in GD2 equates to £8.9m a year and as before, this is a mixture of capital and operational expenditure.

This investment is detailed and justified through twelve accompanying CBAs and engineering justification papers.

6.4 Customer driven investment

This category of projects is characterised by those which are delivering the outcomes relating to maintaining customer service while keeping pace with ever increasing customer expectations and demands. The outputs and details are listed in section 3.4 and the accompanying Engineering Justification paper. At our Moving Forward Together event in London on 14 November 2018, our stakeholders told us better IT online interfaces, both internal and external, are required.

Investment area	Description
Customer and stakeholder solutions	Increased demand driven by customer expectations e.g. increased and varied digital communication channels the use of intelligent agents etc

Our Customer service driven investment in GD2 equates to £0.5m a year and as before, this is a mixture of capital and operational expenditure. This investment is solely to maintain current customer satisfaction levels by addressing the changing and increasing needs and expectations of our customers throughout GD2. We believe that additional investment of c£0.5m a year will support enabling future customer needs to be met as this is based on the level of investment which was made during GD1 to support achieving our levels of customer service and associated customer satisfaction scores.

This investment is detailed and justified in more detail through the accompanying CBA and Engineering Justification Paper.

6.5 Cyber security investment: Business IT security and cyber resilience

UK Government and Ofgem as well as numerous stakeholders and advisors recognise the threat to CNI and UK Utilities in general and the need for a substantial increase in Cyber Security. Given the significant pressure and need to address Cyber Security in a fundamentally different way that of GD2, a discrete and separate section of this report includes the stakeholder evidence supporting this area of activity and funding (See sections 5.2-5.4).

The UK Government and National Cyber Security Centre advises and highlights an ever-increasing risk to the availability of our services, the resilience of our network management, availability of our safety critical gas escape response service and our ability to operate safely and respond to and protect our customer's needs. Section 5.2 provides several references to evidence this.

In addition to this, Ofgem has requested additional reporting and assurance on the EU NIS-Directive which exists to significantly improve Cyber Security capability as well as fine companies who are found to breach this directive. The NIS Directive has been implemented at the same time as the new General Data Protection Regulations (GDPR), which require holders of personal data to provide security assurances around that data, and to report on any incidents that might affect them with the same levels of fines associated with breaches (up to 4% of revenue and/or £17m).

In conjunction with Ofgem and other GDNs, we have received and undertaken an extensive and comprehensive cyber security framework to be reported by us to Ofgem as part of evidence of NIS D compliance. Clearly, this framework, the assessment and the associated cyber security maturity required needs to be linked to the GD2 price control mechanism. Ongoing and future requirements including new and additional reporting requirements, changes in the assessment mechanism, changes in scope and or compliance and enforcement action changes have not been included within our current plans.

We have undertaken extensive analysis to define the most likely areas of investment through the GD2 period and we have obtained advice and input on these plans from numerous external suppliers and advisors. We have also had these plans assessed and assured by Gartner as part of the independent assurance process who have deemed this expenditure to be at the midpoint range of efficiency.

We have detailed our current risk assessment and linked proposed initiatives to each risk as shown within our Cyber Security EJP and accompanying information. We have also provided low-level and very detailed cost estimation information for each initiative to evidence our funding request for GD2.

This paper, the CBA and the associated Business Plan Data Templates (BPDT), have been split as per the guidance from Ofgem, to cover both Business IT Security (IT) and Cyber Resilience (OT). As stated previously, although we have provided this division, the management of cyber security risk within our cpmpany is a shared and centralised function. Therefore, both investment areas need to be looked at in conjunction with each other and cannot be assessed in isolation.

We understand from recent meetings with Ofgem this is in-line with its thinking and separate funding for OT based Cyber resilience is likely to be treated under use-it-or-lose-it arrangements and as a likely reopener.

Our Cyber Security investment in GD2 equates to £4.5m a year and as before, this is a mixture of capital and operational expenditure and OT and IT. When removing OT specific projects and allocating a notional percentage of shared security service investment costs, our Business IT Security investment equates to £3.62m a year and our Cyber Resilience (OT) costs equate to £0.84m a year.

6.6 Future technology readiness investment

Based on best practice advice, and stakeholder consultation, and taking up the recommendations of the Energy Data Taskforce, (see section 5.1) the major areas of technology change in GD2 will be the Industrial internet of things (IIoT) and Analytics, Artificial Intelligence and Machine Learning.

Based on this advice, investment will be required to deal with and utilise IIOT and analytics, AI and machine learning. This investment is not well defined in detail due to the time horizon and expected change in technology, however, it is expected to keep pace with changes to operational technology as well as customer and stakeholder needs, these are areas where we and all GDNs will need to develop tools, technology and process. This will be essential for continuity of service as new technologies impact our business as well as the solutions that are available to us. Resilience and safety will be underpinned by improved connectivity, new data sources and associated insight linked to these.

Investment area	Description
Industrial internet of things	The **Industrial Internet of Things (IIoT**) refers to interconnected sensors, instruments, and other devices, (traditionally defined as Operational Technology), networked together with computers' industrial applications, including, asset and energy management. This connectivity allows for data collection, exchange and analysis
Analytics, artificial intelligence and machine learning	**Analytics** is the discovery, interpretation, and communication of meaningful patterns in data and the process of applying those patterns towards effective decision making. Analytics is the connection between data and effective decision making within an organisation. The areas specifically relevant to us within analytics are; predictive analytics, prescriptive analytics, enterprise decision management, descriptive analytics, cognitive analytics, Big Data Analytics, web analytics, call analytics, and speech analytics **AI** techniques have become an essential part of the technology industry helping to solve many challenging problems. artificial intelligence (AI), sometimes called machine intelligence, is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans. **Machine learning (ML**) is the scientific study of algorithms and statistical models that computer systems use to effectively perform a specific task without using explicit instructions, relying on patterns and inference instead. It is seen as a subset of artificial intelligence

This development has been proven by the numerous innovation projects we have undertaken where connected 'things' have been developed, utilised and either have been, or are in the process of, being rolled-out to our operational environment.

The projects listed in section 5.1 are a sample of IIoT projects delivered under NIA to illustrate and demonstrate the need to develop, support and run these new technologies at scale, safely while addressing the related cyber security risk.

This investment is to support the use of data and analytics internally to run, manage and operate our business more effectively. External provision of this data through, open data and supporting whole systems data analytics have been estimated as part of a separate additional service enhancement offering to customers (section 21.4 of our business plan) and section 6.9 of this appendix.

Our investment in future technology readiness in GD2 equates to on average £1.96m a year capex and £0.3m a year opex.

78% of our stakeholders expect us to utilise the latest technology (reference: SGN Stakeholder Research Report by Impact Utilities. August 2018) yet in the same research, only 38% of our stakeholders believe we are performing well or excelling in utilising the latest technology.

This investment is defined and justified in more detail through the accompanying CBAs and engineering justification papers.

6.7 Volume drivers and reopeners

We note that Ofgem has proposed a reopener for cyber security and agree this is required.

Changes to legislation may require a substantive additional investment to meet the ever-changing needs of this risk. It is also important to note the fast and ever-changing nature of technology may mean that meeting the same or improved levels of Cyber resilience over a long-term time horizon until 2026, may require substantive changes in approach and potential investment requirements to achieve the same level of Cyber resilience expected by Government, Ofgem and customers.

We would propose the reopener should be triggered on a percentage increase or decrease basis over and above cumulative allowances to date based on changes to:

- National or International threat to utilities that require a substantial improvement in cyber security;
- Significant change in third party or activist group and/or exposure of technology third party vulnerabilities that requires an immediate and/or substantive change;
- A major shift in technology adoption (including operational technology) that was not widely anticipated at the time of business plan submission; and
- A significant change in legal or regulatory requirements that warrant a substantial shift in the organisations approach to cyber security.

Cyber resilience and the Cyber Assessment Framework:

It is important to note, due to the timing of publication, our GD2 plans have not incorporated the late and recent changes to Cyber Resilience guidelines and scope definition issued by Ofgem as part of its consultation in October 2019, which is yet to conclude. Therefore, we expect to request a reopener for new, future requirements or the consequential impact of these, including:

- New, additional or significant changes in reporting requirements;
- Changes in the assessment mechanism;
- Changes in scope of the assessment framework and/or its application within distribution networks;
- Changes to inspection, auditing and remediation processes; and
- Compliance and enforcement action changes.

The above have not been included within our current plans and therefore we expect to utilise the reopener mechanism under the above conditions. This would be via the use it or lose it mechanism. We envisage this reopener being initiated by network companies with clear evidence of the above to support any claim. We envisage using this reopener during GD2 in relation to OT Cyber Resilience.

With regards to business IT security, whilst we do not expect to use the reopener mechanism, the nature of this risk is there is a high degree of uncertainty which could affect both network companies and more importantly our customers which may result in a reopener being used in accordance with the other factors listed above.

6.8 Price control deliverable and use-it-or-lose it mechanisms

We do not think a price control deliverable or use-it-or-lose-it mechanisms are appropriate for our IT investment in GD2. We understand Ofgem wishes to apply a use-it-or-lose-it mechanism specifically to Cyber Resilience (OT) investment.

6.9 Additional strategic outputs: Stakeholder-led additional requirements and outputs

Two additional strategic options have been identified:

- Providing open data capability as part of the strategic direction set by the Energy data task force and the associated Ofgem guidance around digitalisation; and
- Utilising smart meter data through DCC membership.

6.9.1 Modernising energy data: Open data and whole energy system analytics

The Government and Ofgem have commissioned reports from think tanks Catapult, Energy Data Taskforce: A Strategy for a Modern Digitalised Energy System and the Energy Technologies Institute Energy Data Review: Data for the Public Good. These reports highlight the need to modernise and digitise the energy system and the key role data and technology play in delivering innovation across the energy system of the future. In response to this, we have also received guidance from Ofgem on defining our digitalisation strategy, which will be required to support and develop the recommendations of the EDTF and wider energy system modernisation.

Big data, open/shared data, analytics, machine learning and artificial intelligence, all offer transformational opportunities. Unlike our investment case for Analytics, AI, ML and DL, the need to invest in open data and whole energy system analytics is driven by the need to present and share our digitalised data externally and for purposes that we do not currently do as of today under as part of our regulatory outputs and licence to operate.

In response to this, we have defined our own digitalisation strategy which outlines our approach to digitalisation of our network infrastructure and assets and calls out the importance of data and technology in delivering EDTF’s recommendations. This is published on our website in-line with Ofgem’s guidance.

Also in-line with this guidance received from Ofgem and EDTF around digitalisation, we have seen increasing expectation and pressure to share our data with other entities outside our current operations and obligations for the benefit of customers and stakeholders.

We have provided a cost estimate of £750k a year capex cost and £300k a year opex to provide suitable IT platforms and changes to meet the needs defined by these important stakeholders. These costs have been derived based on our historical costs to build and utilise our other analytics platforms.

We have defined and justified this expenditure in more detailed within the associated Engineering Justification Paper and Cost Benefit Analysis and this investment area has been independently assessed by Gartner.

We are pleased to see the commitment from Ofgem to work closely with industry and other stakeholders in supporting this work and the recognition that changes to the RIIO-2 framework of funding and incentives may become necessary to support the delivery of high-quality digitalisation strategies.

6.9.2 Smart metering DCC (Data Communications Company): Set-up and ongoing membership

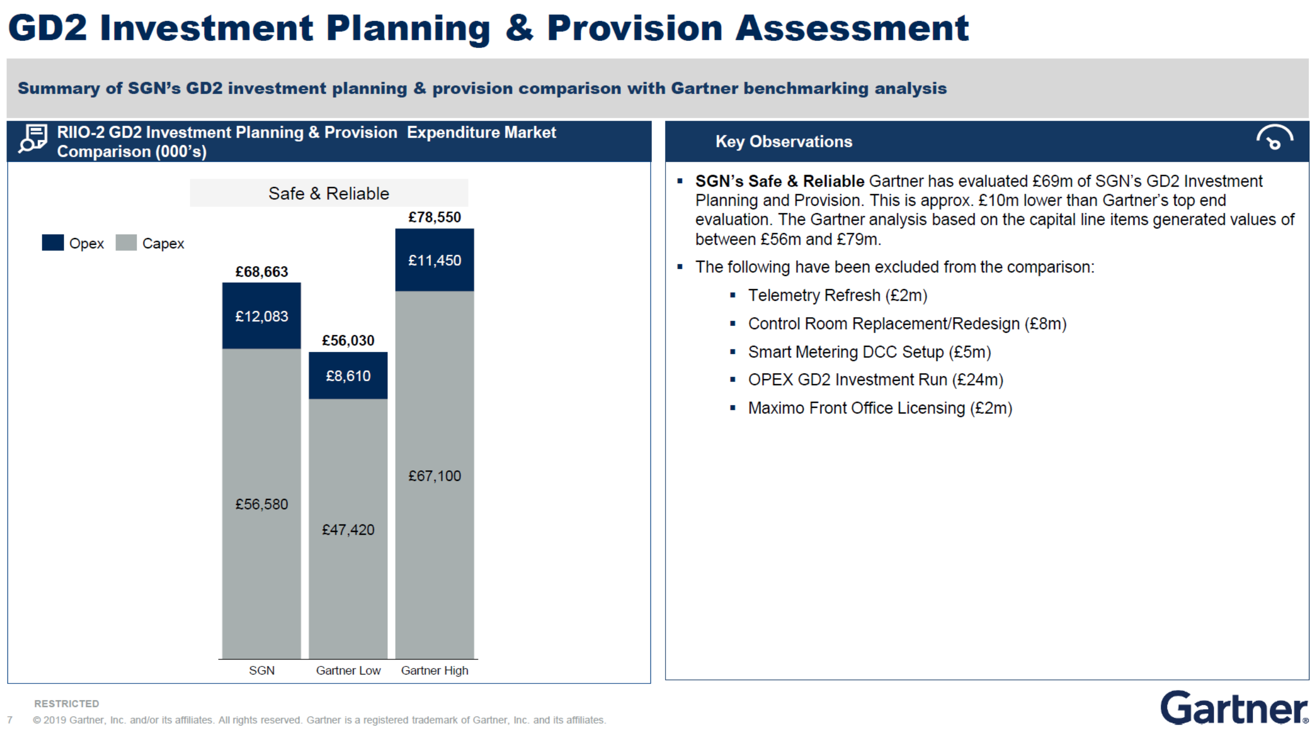
The UK government has indicated there may be an expectation for GDNs to invest in utilising consumption data being provided by smart meters in order to improve the management of shrinkage, leakage, theft of gas and forecasting. We have also received feedback from our Customer Engagement Group and the Customer Challenge Group that they expect to see us make use of smart metering data.

While we remain unconvinced of the benefits of this data today in managing our network and to our customers (as opposed to suppliers’ customers) due to the level of aggregation, anonymisation and timeliness of data provision, we will keep an open mind and frequently reassess and test the opportunity for benefits to customers in our use of smart meter data.

We have therefore, provided indicative costs to implement the necessary data platform, designing and setting up systems and the associated interfaces to interact with the DCC plus, the ongoing cost of DCC membership as derived from published price lists. Our Customer Engagement Group advised it would expect GDNs to make use of smart meter data. We estimate this will require a £5m capital investment followed by an ongoing cost of £0.1m a year. A more detailed Engineering Justification Paper and CBA has been produced to define the pros and cons of this investment in more detail.

6.10 Cost assessment

An independent assessment and review of our investment costs is particularly important for areas relating to long-term future technology readiness as defined in the previous section. We have undertaken an independent assessment of all IT run and investment projects, this identified our investment plans are in-line with the expected range and between the lower and higher ranges as shown below.



GD2 Investment Planning & Provision Assessment

Summary of SGN's GD2 investment planning & provision comparison with Gartner benchmarking analysis

RIIO-2 GD2 Investment Planning & Provision Expenditure Market Comparison (000's)

Key Observations

- **SGN's Safe & Reliable** Gartner has evaluated £69m of SGN's GD2 Investment Planning and Provision. This is approx. £10m lower than Gartner's top end evaluation. The Gartner analysis based on the capital line items generated values of between £56m and £79m.
- The following have been excluded from the comparison:
  - Telemetry Refresh (£2m)
  - Control Room Replacement/Redesign (£8m)
  - Smart Metering DCC Setup (£5m)
  - OPEX GD2 Investment Run (£24m)
  - Maximo Front Office Licensing (£2m)

RESTRICTED

7 © 2019 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner

The key factors considered when deriving these plans are:

- There is a significantly increased technology adoption across all aspects of our business when compared to the first half of GD1 and this is a trend we know will continue throughout GD2 as validated by Gartner and as is the case across all sectors and industry;
- An exponential increase in Cyber Security threat on Gas networks. GD1 expenditure demonstrated a year-on-year increase of 40% when compared to the initial GD1 allowances (£4.5m a year average and £22.3m across five years);
- A significantly increased dependence on data, information, analytics and insight to run our business safely and resiliently during 2021 to 2026 and a major shift and reliance on an ever increasing smart and connected network aka Industrial Internet of Things (IIoT); and
- Ongoing 'Run' costs (opex) movement from c. £29.5m a year in the final four years of GD1 to £32.8m a year average across GD2. This increase reflects the additional average cost of £4.2m a year to run additional services identified as areas for investment and driven by the same factors listed above.

The efficiency and accuracy of our future investment costs has been demonstrated by Gartner analysis and research information provided within our separate assurance and benchmarking report.

Detailed phasing of investment cost profiles is defined and justified in the accompanying CBAs and engineering justification papers.

6.11 Engineering Justification Papers (EJPs)

Each Engineering Justification Paper (EJP) and associated Cost Benefit Analysis (CBA) we produce seeks to meet and answer the framework set by Ofgem. Although the structure and format of these documents and templates are not entirely suited to IT and Cyber security investment, we have not deviated from this structure or format.

Each EJP has undergone a validation and verification process with both peer and independent review and each cost area has been independently assessed by Gartner as part of our assurance process. There has been substantive external, expert advice used in assessing and defining these papers as outlined previously in this document. This allows us to ensure there is a high level of confidence in the assurance process for these EJPs.

For each project and area of investment an EJP and CBA has been completed which defines the problem and consequences of failure, analyses the options available and provides technical solutions and the rationale behind the justification.

IT investment projects

Network	Asset	Total Value £m	NPV	Payback	Engineering Justification Paper
SC & So	Application Refresh	2.5	108	3	SGN IT - 001 AppRef EJPDec19
SC & So	Back Office Replacement or Redesign	4.0	102	3	SGN IT - 002 BO EJPDec19
SC & So	Business as Usual Consumables & Break-Fix Devices	6.1	95	3	SGN IT - 003 BAU EJPDec19
SC & So	Comms Refresh	6.0	96	3	SGN IT - 004 Comms EJPDec19
SC & So	Control Room Replacement or Redesign	8.0	88	3	SGN IT - 005 ContRm EJPDec19
SC & So	Customer Experience & Stakeholder	2.5	1	15	SGN IT - 006 CustSk EJPDec19
SC & So	Cyber Investment	22.3	75	3	SGN IT - 007 Cyber EJPDec19
SC & So	Data Governance And Quality	0.5	Opex only	-	SGN IT - 008 DataGov EJPDec19
SC & So	DCC Membership	5.5	-13	50	SGN IT - 009 DCC EJPDec19
SC & So	Device Refresh	6.0	95	3	SGN IT - 010 DevRef EJPDec19
SC & So	Financial Planning And Reporting Tools	0.5	95	4	SGN IT - 011 FinPlan EJPDec19
SC & So	Front Office Replacement or Redesign	6.0	95	3	SGN IT - 012 FO EJPDec19
SC & So	Future Technology Readiness - Analytics, AI And ML	5.0	99	21	SGN IT - 013 AI EJPDec19
SC & So	Future Technology Readiness - IIOT, Ot/It, Remote Comms	6.3	95	3	SGN IT - 014 IIOT EJPDec19
SC & So	Integration Including Replacement / Refresh	1.1	114	3	SGN IT - 015 Integ EJPDec19
SC & So	Open Data	5.3	20	3	SGN IT - 016 OpenData EJPDec19
SC & So	Regulatory & Mandatory Change	2.0	95	3	SGN IT - 017 RegChg EJPDec19
SC & So	Telemetry Refresh	2.0	110	3	SGN IT - 018 Telem EJPDec19
		91.6	**1368.5**		

6.12 Assurance

Our business plan, including appendices, has been subject to a rigorous assurance process which is detailed in Chapter 3 of the Plan and the Board Assurance Statement.

Our Director of IT & innovation was appointed as the Sponsor for the IT appendix and the associated Cost Benefit Analyses (CBAs), Engineering Justification Papers (EJPs) and Business Plan Data Templates (BPDTs); which have been through the following levels of review and assurance:

First line

This was undertaken at project level by the team producing the document, as a regular self-check or peer review.

Second line

This was undertaken independently within the organisation to review and feedback on product development, including a workshop on IT and Cyber Resilience. Both Senior Manager and Director sign-off was obtained.

Our GD2 Executive Committee: (1) considered the appropriateness of assurance activity for the Appendix and (2) provided assurance to SGN's Board that the Business Plan meets Ofgem's assurance requirements.

Third line

This was undertaken by external advisors and groups providing critical challenge during the development of products within the Business Plan. Feedback and challenge were provided by the Customer Engagement Group (CEG) and Customer Challenge Group (CCG).

Fourth line

This was undertaken by independent and impartial external providers, who provided a detailed and comprehensive report to both the Executive Committee and Board of Directors:

Advisor/group	Contribution
Gartner	IT cost benchmark and capital programme review
PwC	Business plan data template review: IT and telecoms group and other capex

6.13 Funding rationale

For the purposes of the business plan submission we have made our forecast on the following assumptions:

- The two strategic, stakeholder driven options identified above are included within the current cost estimates;
- These cost assessments include IT and Telecoms expenditure;
- Capex/opex split for investment is not comparable to GD1;
- The costs are with Scotland and Southern combined. This is how we operate and run IT for efficiency purposes;
- All third-party prices (software, hardware and service charges) are presumed to be flat with only inflation applied i.e. we have not factored in any risk provision for price rises and market volatility;
- Although our cyber security costs submission has been separated between Business IT Security (IT) and cyber resilience, as guided by Ofgem, our management of cyber risk, the delivery of improved capability and security services is centralised and shared. For this reason, it is imperative both areas of investment are looked at jointly and not in isolation. Cyber resilience (OT) and the associated investment plan will be subject to use-it-or-lose-it mechanism and as part of a reopener mechanism outlined in section 6.7, we expect to provide fuller and more defined cyber resilience (OT) plans as these requirements develop. We understand from recent meetings with Ofgem this is in-line with its thinking on how to approach OT cyber resilience and we will continue to work closely with this team to refine our plans collaboratively.

All costs have been independently benchmarked by Gartner as part of our fourth line assurance. Additionally, all data templates have been independently assured by PwC.

7 Conclusion

As set out above, the costs in the table below are separated according to the main cost categories of:

- **Mandatory IT Investment** - Additional investments that are required to keep IT asset health at a constant level to our level today and ensure continuity of service. This includes Statutory, legal and regulatory change;
- **Customer driven investment** - Projects that are necessary to maintain current levels of customer service while we keep pace with increasing customer expectations and demands;
- **Cyber Security (Business IT Security and Cyber Resilience)** - Additional investment in cyber security to address the ever-increasing Cyber Risk and comply appropriately with legislation and mitigate the risk of a fine or penalty being imposed;
- **Future technology Readiness** - Additional investment in keeping up to date with specific industrial and IT trends to deliver the level of customer service and analytical capability expected by our customers and stakeholders;
- **Additional Outputs** - Stakeholder led additional requirements and outputs. Providing open data capability and utilising smart meter data through DCC membership; and
- **IT Run Costs** - These are split out below into investment, licencing, ongoing costs and employee costs.

In the table below, we have combined the capex and the opex lines, these are split out in the business plan data templates appropriately.

Table 3: IT investment costs (capex and opex costs – pre-allocation)

IT capex costs (Investment/projects only)													
SGN (£m)	**13/14**	**14/15**	**15/16**	**16/17**	**17/18**	**18/19**	**19/20**	**20/21**	**21/22**	**22/23**	**23/24**	**24/25**	**25/26**
Mandatory IT	13.12	23	13.07	7.01	16.33	13.08	11.59	4.94	9.40	9.25	9.36	7.83	7.11
Mandatory business	-	-	-	-	-	-	-	-	0.25	0.25	0.25	0.25	0.25
Business IT security	-	-	-	-	-	-	-	-	1.85	2.16	1.45	3.04	3.65
Cyber resilience	-	-	-	-	-	-	-	-	0.21	0.24	1.39	0.34	0.41
Future technology Readiness	-	-	-	-	-	-	-	-	1.82	1.50	1.55	1.94	2.99
DCC membership	-	-	-	-	-	-	-	-	0.50	0.50	1.50	1.50	1.00
Open data	-	-	-	-	-	-	-	-	1.00	0.75	0.75	0.50	0.75
Total capex	**13.12**	**23.00**	**13.07**	**7.01**	**16.33**	**13.08**	**11.59**	**4.94**	15.03	14.66	16.25	15.40	16.16
IT opex costs (Run and investment)													
Mandatory IT	-	-	-	-	-	-	-	-	0.50	0.25	0.50	0.25	0.25
Mandatory	-	-	-	-	-	-	-	-	0.25	0.25	0.25	0.25	0.25

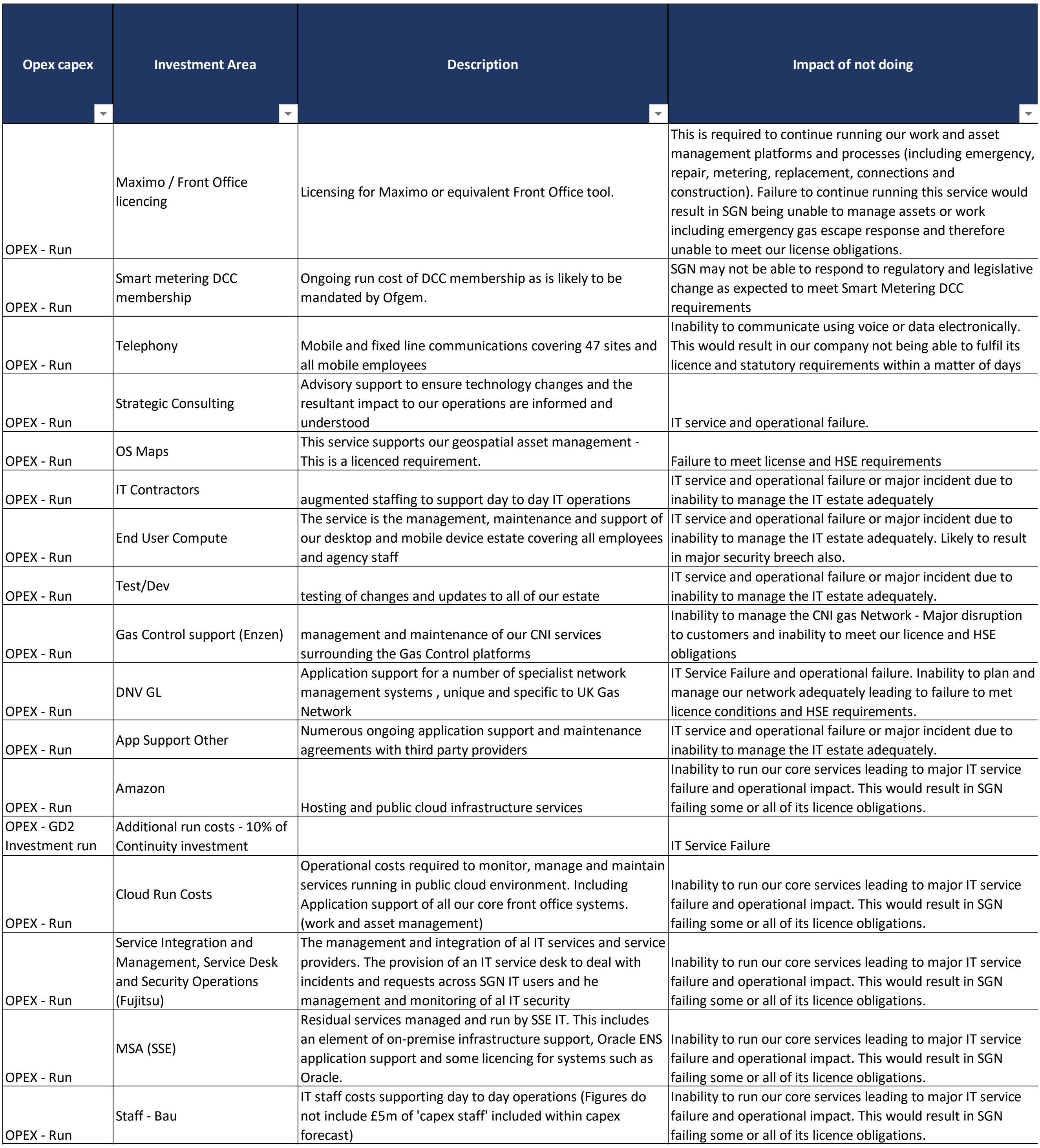
business													
Investment run	-	-	-	-	-	-	-	-	0.98	2.37	3.70	4.96	6.30
Business IT security	-	-	-	-	-	-	-	-	0.43	0.59	1.30	1.62	2.03
Cyber resilience	-	-	-	-	-	-	-	-	0.50	0.57	0.14	0.18	0.23
Future technology Readiness	-	-	-	-	-	-	-	-	0.10	0.10	0.20	0.50	0.60
DCC membership	-	-	-	-	-	-	-	-	0.10	0.10	0.10	0.10	0.10
Open data	-	-	-	-	-	-	-	-	0.30	0.30	0.30	0.30	0.30
Licencing	-	-	-	-	-	-	-	-	0.40	0.40	0.40	0.40	0.40
Ongoing cost	21.16	22.62	24.09	27.33	27.66	36.9	33.09	29.23	21.64	22.26	22.26	22.26	22.26
Employees	-	-	-	-	-	-	-	-	6.56	6.56	6.56	6.56	6.56
Total opex (Run)	**21.16**	**22.62**	**24.09**	**27.33**	**27.66**	**36.90**	**33.09**	**29.23**	**31.75**	**33.74**	**35.71**	**37.38**	**39.27**

8 Glossary

All acronyms and associated descriptions can be found within the Glossary appendix.

9 Annex

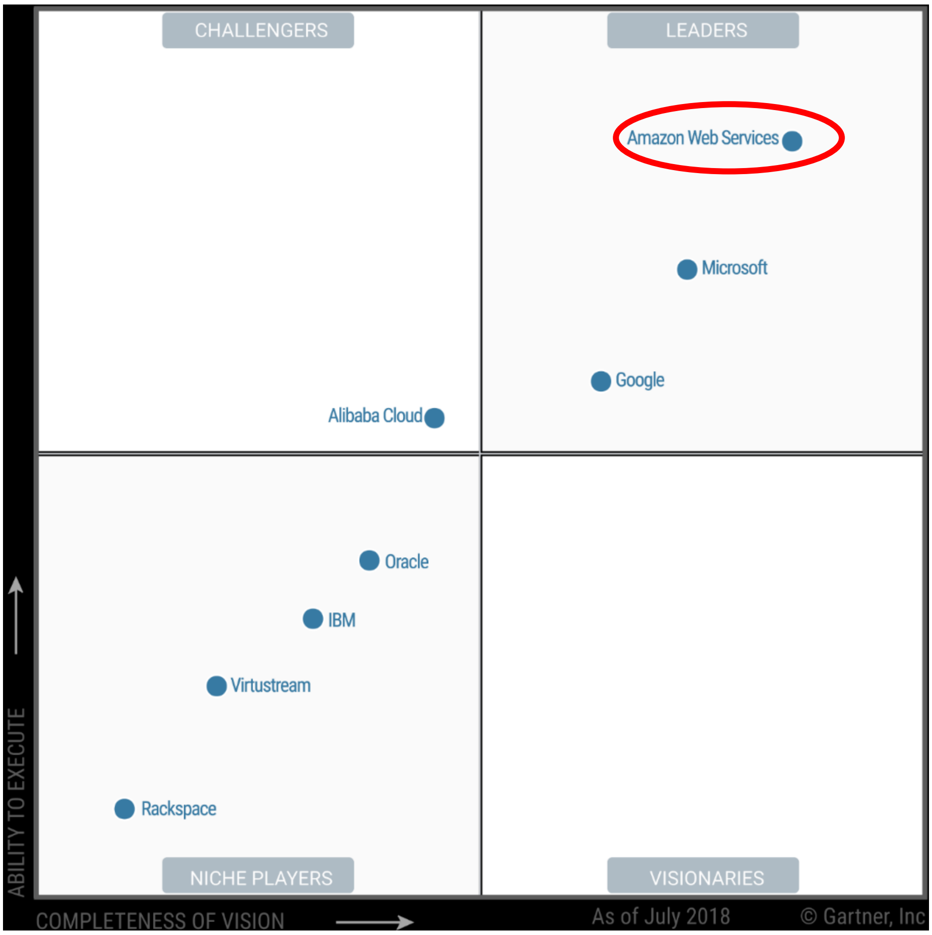
1. IT run services



Opex capex	Investment Area	Description	Impact of not doing
OPEX - Run	Maximo / Front Office licencing	Licensing for Maximo or equivalent Front Office tool.	This is required to continue running our work and asset management platforms and processes (including emergency, repair, metering, replacement, connections and construction). Failure to continue running this service would result in SGN being unable to manage assets or work including emergency gas escape response and therefore unable to meet our license obligations.
OPEX - Run	Smart metering DCC membership	Ongoing run cost of DCC membership as is likely to be mandated by Ofgem.	SGN may not be able to respond to regulatory and legislative change as expected to meet Smart Metering DCC requirements
OPEX - Run	Telephony	Mobile and fixed line communications covering 47 sites and all mobile employees	Inability to communicate using voice or data electronically. This would result in our company not being able to fulfil its licence and statutory requirements within a matter of days
OPEX - Run	Strategic Consulting	Advisory support to ensure technology changes and the resultant impact to our operations are informed and understood	IT service and operational failure.
OPEX - Run	OS Maps	This service supports our geospatial asset management - This is a licenced requirement.	Failure to meet license and HSE requirements
OPEX - Run	IT Contractors	augmented staffing to support day to day IT operations	IT service and operational failure or major incident due to inability to manage the IT estate adequately
OPEX - Run	End User Compute	The service is the management, maintenance and support of our desktop and mobile device estate covering all employees and agency staff	IT service and operational failure or major incident due to inability to manage the IT estate adequately. Likely to result in major security breech also.
OPEX - Run	Test/Dev	testing of changes and updates to all of our estate	IT service and operational failure or major incident due to inability to manage the IT estate adequately.
OPEX - Run	Gas Control support (Enzen)	management and maintenance of our CNI services surrounding the Gas Control platforms	Inability to manage the CNI gas Network - Major disruption to customers and inability to meet our licence and HSE obligations
OPEX - Run	DNV GL	Application support for a number of specialist network management systems , unique and specific to UK Gas Network	IT Service Failure and operational failure. Inability to plan and manage our network adequately leading to failure to met licence conditions and HSE requirements.
OPEX - Run	App Support Other	Numerous ongoing application support and maintenance agreements with third party providers	IT service and operational failure or major incident due to inability to manage the IT estate adequately.
OPEX - Run	Amazon	Hosting and public cloud infrastructure services	Inability to run our core services leading to major IT service failure and operational impact. This would result in SGN failing some or all of its licence obligations.
OPEX - GD2 Investment run	Additional run costs - 10% of Continuity investment		IT Service Failure
OPEX - Run	Cloud Run Costs	Operational costs required to monitor, manage and maintain services running in public cloud environment. Including Application support of all our core front office systems. (work and asset management)	Inability to run our core services leading to major IT service failure and operational impact. This would result in SGN failing some or all of its licence obligations.
OPEX - Run	Service Integration and Management, Service Desk and Security Operations (Fujitsu)	The management and integration of al IT services and service providers. The provision of an IT service desk to deal with incidents and requests across SGN IT users and he management and monitoring of al IT security	Inability to run our core services leading to major IT service failure and operational impact. This would result in SGN failing some or all of its licence obligations.
OPEX - Run	MSA (SSE)	Residual services managed and run by SSE IT. This includes an element of on-premise infrastructure support, Oracle ENS application support and some licencing for systems such as Oracle.	Inability to run our core services leading to major IT service failure and operational impact. This would result in SGN failing some or all of its licence obligations.
OPEX - Run	Staff - Bau	IT staff costs supporting day to day operations (Figures do not include £5m of 'capex staff' included within capex forecast)	Inability to run our core services leading to major IT service failure and operational impact. This would result in SGN failing some or all of its licence obligations.

2. Gartner magic quadrant extracts relating to SGN IT services

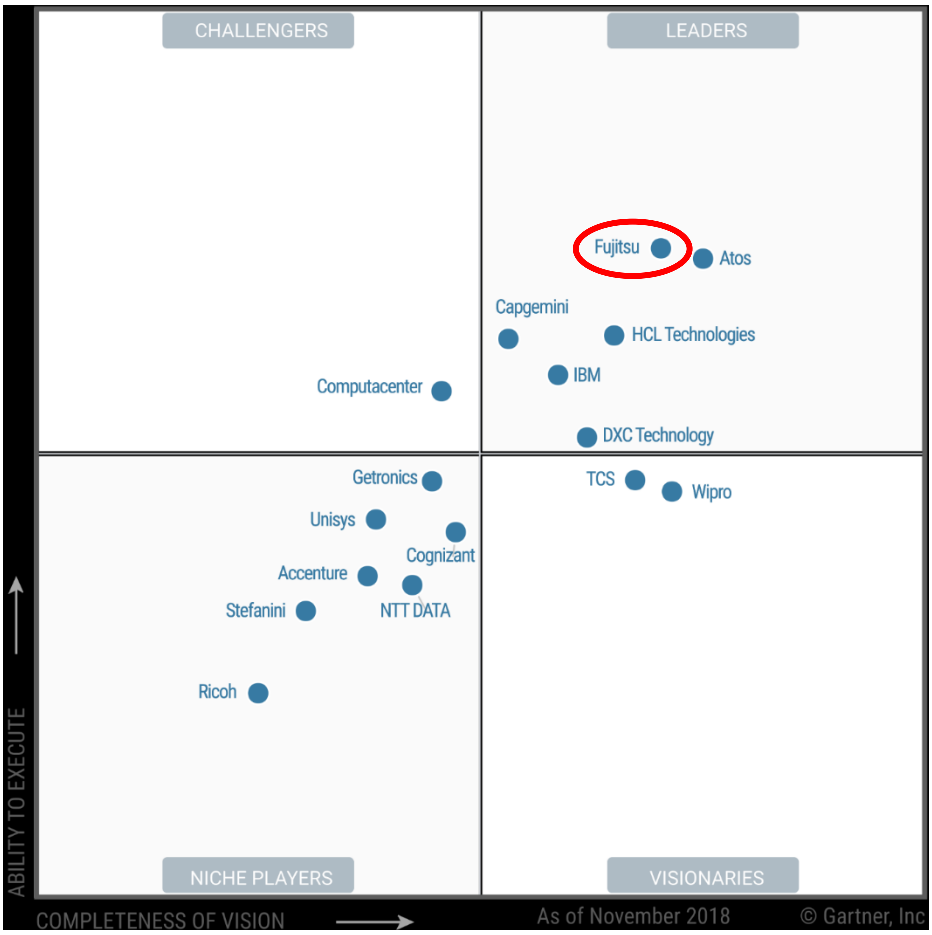
Magic Quadrant for Public Cloud Storage Services, Worldwide: Published 31 July 2018



Amazon Web Services: Strengths

- Amazon S3 is the category leader in terms of revenue and amount of data under management. The overwhelming dominance of the Amazon S3 API gives AWS control of both the ecosystem of developers who use the S3 API, but also the storage vendors who implement the S3 API in their storage products delivered on-premises.
- Customers use AWS's storage services for a broad range of workloads, from cloud-native to traditional enterprise applications. Relatedly, AWS is often on the shortlist for Windows and Oracle applications.
- AWS is one of the few capable providers that can provide end-to-end solutions from edge and on-premises enterprise data centers to public cloud storage services without making security trade-offs. AWS can deliver such solutions in an integrated experience with an overlay consisting of robust security and performance features.

Magic Quadrant for Managed Workplace Services, Europe: Published 14 January 2019



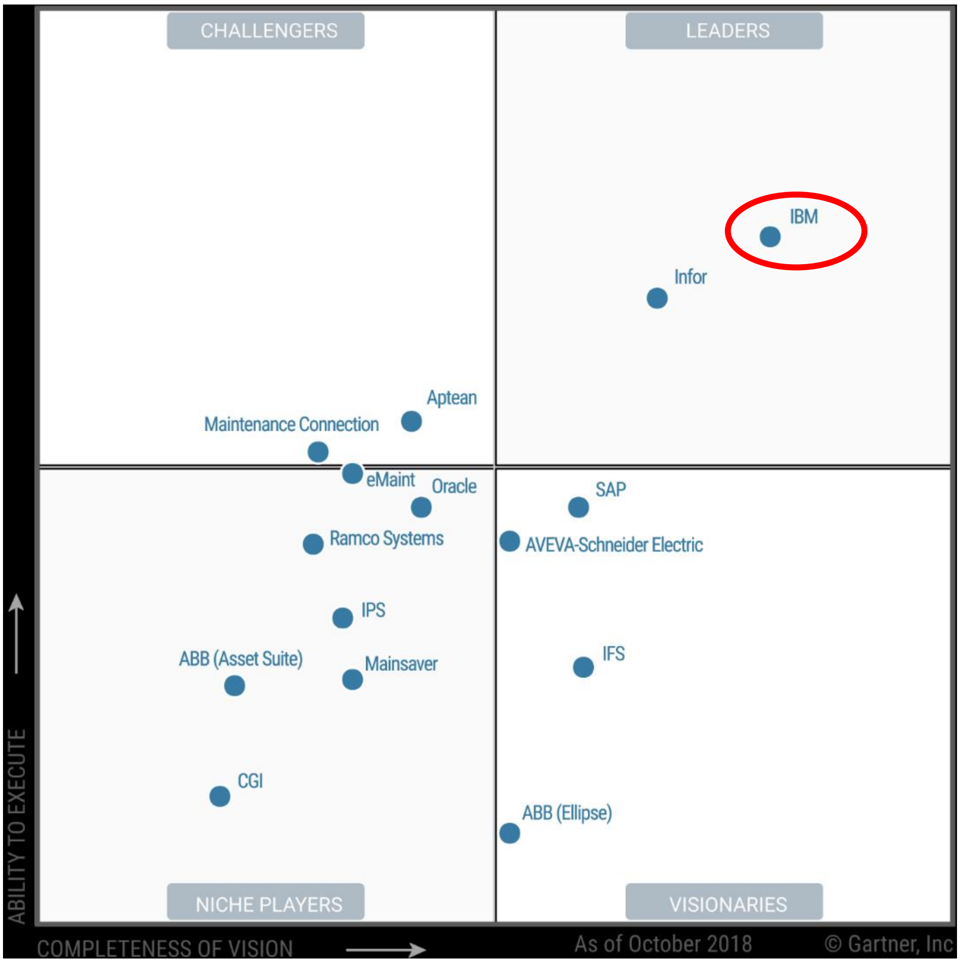
Fujitsu: Strengths:

- Fujitsu's Human Centric Innovation (for responsible digital innovation) looks at the impact of digital on society and embeds an ecosystem concept across customers, partners, start-ups and academia. This approach supports outcomes like BuddyConnect, a mobile app to help new joiners, with extra support for users with learning disabilities or autism. Its service roadmap for consumer-like solutions which integrate personal and work-life encompasses cognitive insight across all services and a simplified, automated digital user experience underpinned by a smart fabric of applications. To support this transformation, Fujitsu is investing significantly in reskilling staff, with 20,000 staff currently being trained in agile delivery.

- It delivers end-user computing via Workplace Anywhere, supporting cloud, hybrid and virtual desktops, O365 and Google G Suite. Its Social Command Centre drives productivity through self-service and AI, while its Intelligent Engineering provides secure, proactive delivery of hardware and on-site support. Its Digital Transformation Centre enables co-creation of new workplace services, which Fujitsu will underwrite through business outcomes such as increased user productivity. Fujitsu has automated the resolution of 18% of calls to its service desk and has used this to actively reduce the number of employees on its service desk.

- Some references praised for Fujitsu for the technical skills of its employees and the quality of its service desk. They appreciated the ability to also access scarce skills from deeper within Fujitsu, as well as its ability to influence industrywide thinking. They also valued Fujitsu's ability to understand their needs, the quality of its deskside support and its value for money.

Magic Quadrant for Enterprise Asset Management Software. Published 9 October 2018

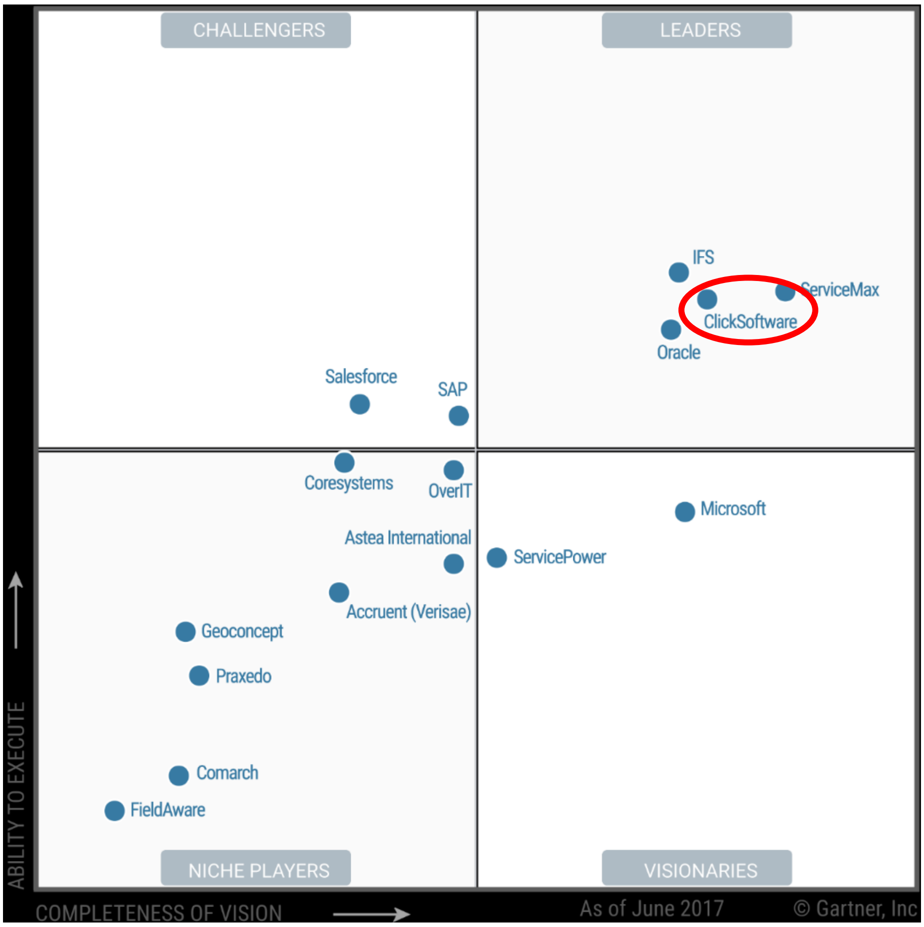


IBM: Strengths

- Maximo is a highly scalable product with a large global customer base.
- A high proportion (70%) of customers are on the latest software release, indicating good customer commitment to the product.
- Maximo has a long history in the market and has built a significant implementation partner network with particular experience in oil and gas, manufacturing, and utilities.
- Over time, IBM has developed an extensive ecosystem of third-party extensions to expand basic functionality in areas such as mobility, planning and APM.
- The product is suitable for both small and very large enterprises, though smaller organizations may be overwhelmed by the complexity given the scope of functionality that has been developed over decades.
- The product supports a broad range of functionality across all industry subsectors using industry extensions.

- IBM customer references give high ratings to their overall experience, dealing with the vendor, its effectiveness in solving problems and meeting client needs, and third-party consulting and integration resource availability.
- The Maximo product scores well for quality of product, functional capabilities, reliable and bug-free software, ease of integration using standard APIs, overall integration, and product deployment.
- The company has strong involvement with industry trends such as PAS 55 and ISO 55000 support and certification, as well as the technical controls that support 21 CFR Part 11 compliance.

Magic Quadrant for Field Service Management. Published 27 September 2017

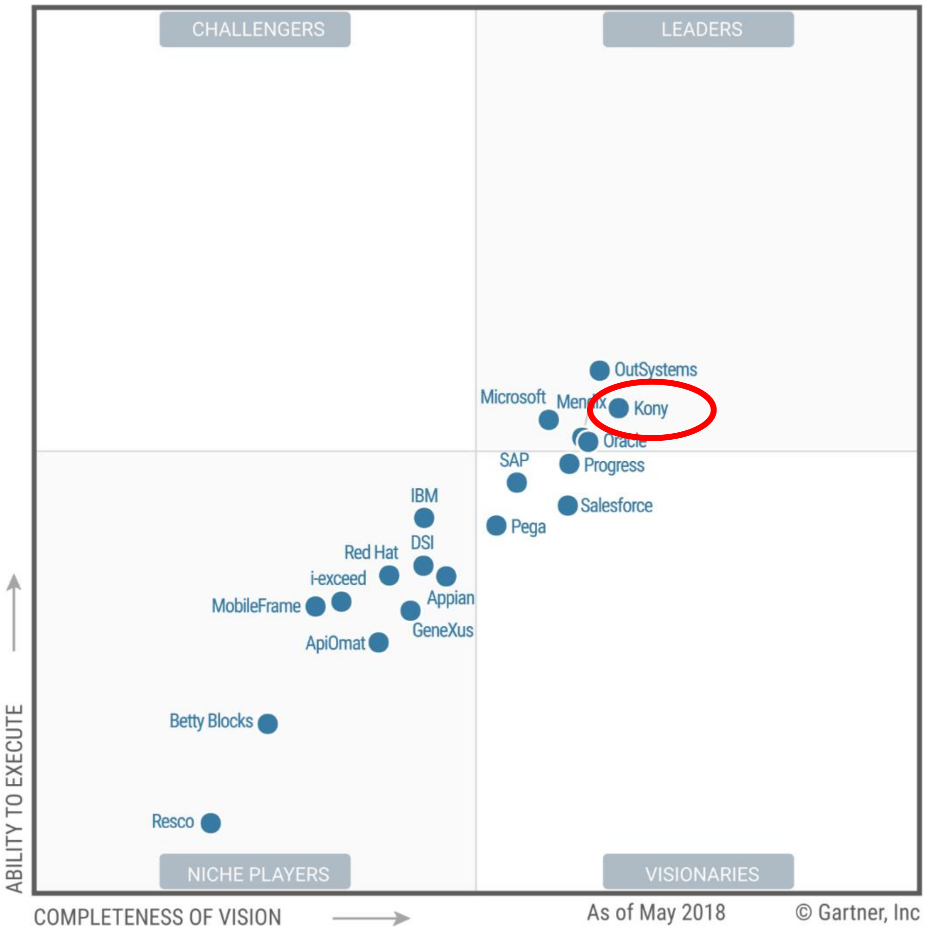


ClickSoftware: Strengths

- **Product ecosystem:** ClickSoftware offers advanced functionality through OEMs and partnerships, such as predicted traffic for scheduling (Google), remote support and augmented reality (Fieldbit) and packaged IoT integration (IBM [Bluemix], ThingSpeak). Its functionality is also sold as part of other vendors' solutions, such as those of Salesforce (Field Service Lightning), SAP (which recently added CFSE to a solution extension partner agreement that it already had for SO Suite) and ServiceBench (a reseller agreement), as well as through system integrators (SIs).
- **Product depth and mobile platform:** Business analysts can use ClickSoftware's Mobility Studio to extend and modify its hybrid HTML5 and native application, and/or employ developers to build new applications, logic and flows.

- **Innovation:** ClickSoftware's outcome-based Optimize to Goals dashboards enable users to perform simulations using slider bars to change weightings for competing outcomes such as cost of service, SLA and customer satisfaction. Future versions will employ artificial intelligence (AI) and parallel simulations to help prioritize the hundreds of configurations that support each outcome.
- **Market responsiveness:** ClickSoftware's approximately 700 employees and long market tenure help it react well to market shifts. Recent introductions by ClickSoftware, such as chatbots, an AI dispatcher (which proactively prevents predicted SLA breaches) and "soft" service area boundaries, are helping it to lead the market.

Magic Quadrant for Mobile App Development Platforms. Published 17 July 2018



Kony: Strengths

- Kony is again a Leader. One of the original MADP vendors, Kony continues to expand the capabilities of its platform in the web app development arena, and therefore has emerged as a competitor in the high-productivity application platform as a service (hpaPaaS) segment. Kony has a healthy number of MADP customers (over 550), half of them being large enterprises.
- Product offering: Kony's MADP offers one of the most comprehensive cross-platform development environments. Reference customers indicated above-average overall satisfaction with Kony's MADP, in comparison to those of other vendors in this Magic Quadrant. In addition, Kony Fabric back-end services

are very competitive in the overall application platform as a service (aPaaS) market, spanning both web and mobile development.

- Market understanding: Kony continues to add capabilities beyond mobile apps that support some of the key functions demanded by the market, such as conversational and AI-driven capabilities. The company has also enhanced its training enablement with Kony Base Camp, an online community for developers.
- Industry strategy: Kony has strong partnerships with industry partners like CDW, Diebold Nixdorf, SoftBank and Tech Data (Avnet), which have given it new access to financial services, retail, energy/utilities and healthcare markets. Kony also offers pre-packaged digital banking SaaS applications on top of its platform, which enable it to target business buyers in the banking sector.

Magic Quadrant for Analytics and Business Intelligence Platforms Published 11 February 2019

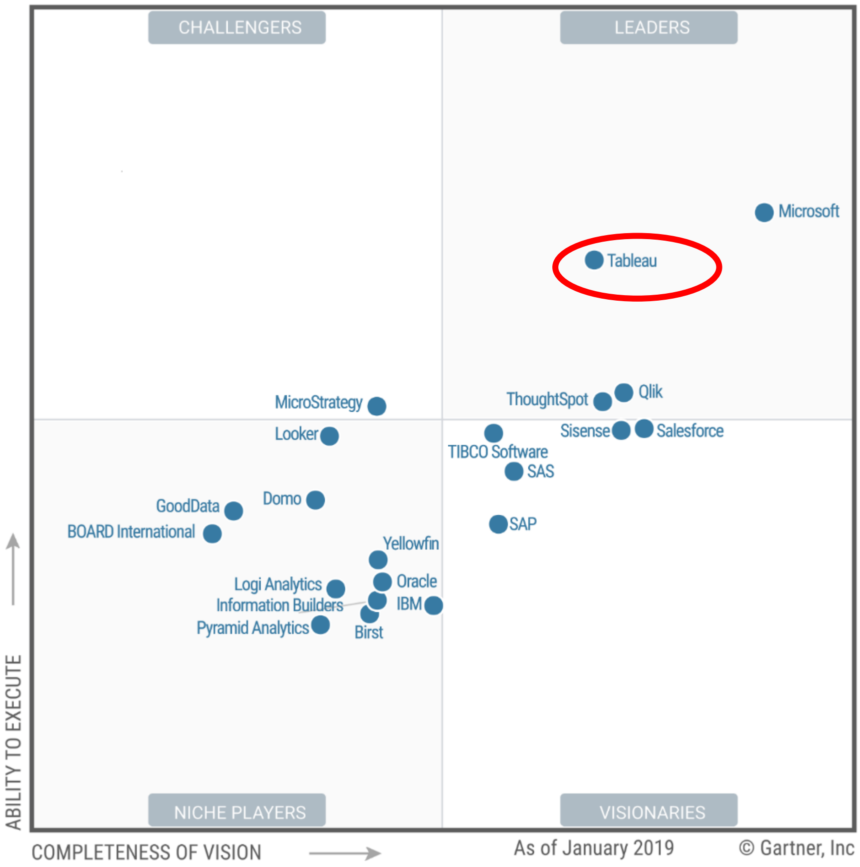


Tableau: Strengths

- **Easy visual exploration and data manipulation:** Tableau enables users to rapidly ingest data from a broad range of data sources, blend them, and visualize results using best practices in visual perception. Data can be manipulated while visualizing - such as when creating groups, bins and new hierarchies - all with a high degree of ease of use.
- **Customers as fans:** Customers have a fanlike attitude toward Tableau, as evidenced by the record 17,000 users that attended its 2018 annual user conference. Reference customers placed Tableau in the top third of Magic Quadrant vendors for customer experience and gave it high scores for achievement of business benefits. Tableau sets the industry standard for user enablement with Meetup groups, roadshows, online tutorials and availability of skills in the market.

- **Momentum:** Tableau grew its total revenue to just over $800m through 3Q18 - double-digit growth compared with 2017. This was despite moving to subscription-based licensing, which often impairs a vendor's growth. Tableau remains at the top of many customers' shortlists and continues to expand within its installed base. The Tableau Foundation and Tableau Public have been a force in the Data for Good movement, having recently pledged $100m in funding over the next seven years.