



IT and Telecoms Strategy

December 2024



Contents

Executive Summary	1
SGN IT and Telecoms Strategy	3
Section A Introduction	3
Purpose and Scope	4
SGN’s Evolving Digital Landscape	4
SGN’s GD2 Technology Transformation	5
SGN’s GD3 Investment Plans	6
The SGN Estate	12
Enterprise Architecture-led Approach and Assessment Processes	14
Section B Networks and Telephony	15
Overview	15
SGN’s Objectives for GD3	15
GD3 Roadmap	16
Section C End User Compute	17
Overview	17
SGNs Objectives for GD3	17
GD3 Roadmap	18
Section D Applications and Cloud	18
Overview	18
SGN’s Objectives for GD3	20
Roadmap for GD3	22
Maintenance of SGN’s Cloud Estate	24
Section E Conclusions and Assurance	24
Appendix: Glossary of Terms	25

Executive Summary

- 1 Within our overarching GD3 Business plan, our core commitments have been shaped by our most extensive engagement programme ever, with input and constructive challenge from our customers and the many stakeholders we work alongside locally and nationally. Our safety critical, 24x7, CNI operations with associated licence conditions and output delivery, the secure and resilient supplies and the best in class, high quality customer service we provide, as described within our business plan, are completely dependent upon the IT and Telecoms services outlined within this strategy document as well as the justification for each area which is detailed within the supporting justification papers referenced within this document. Within our core plan we have listed 22 commitments. While all of these are supported by our IT and Telecoms strategy in some way, three are directly an outcome of the delivery of this strategy and associated funding.
- 2 Directly linked Business Plan Commitments.
 - [REDACTED]
 - [REDACTED]
 - **Commitment 20** - We will open our data to facilitate collaborative planning and the development of whole-system solutions.
- 3 These commitments are outlined within Chapter 3 of our business plan and this IT and Telecoms Strategy, in addition to our published SGN Digitalisation Strategy¹ and the Network Information Systems Annual Report² provide additional detail on how these will be delivered.
- 4 SGN's IT systems services and infrastructure underpin our ability to provide emergency response, network operations and asset management to ensure a safe and secure network, protecting life and property, to serve our customers and other stakeholders and to add social value by innovating and sharing data. The digital landscape in which our IT infrastructure operates has evolved markedly over the past few years. This evolution is driven by technological advancements, shifting business needs, new ways of working and emerging global trends. SGN's IT needs to evolve in line with these shifts to ensure it remains fit for purpose and enables us to adapt to an increasingly dynamic and changing energy landscape and remain secure and resilient to emerging disruptors. IT systems and networks also underpin and enable operational efficiency by providing the means to converge, simplify, standardise and automate core business processes. This relies on robust operational platforms and networks, capacity and bandwidth to support increased data flows, and capable end user devices. There is considerable integration between this IT and Telecoms Strategy, the SGN Digitalisation Strategy, and the SGN Cyber Investment and Governance Strategy and action plan.
- 5 Over the last four years, SGN has commenced on a major IT transformation. Our primary driver is always to provide the best technology services that enable and protect our people and serve our customers. Our goals of this transformation have been to: Improve resilience and availability (current target 99.52% service uptime within defined service hours), improve security, increase agility, reduce costs and align to innovation and new ways of working. We have invested significantly in technology, processes, and people to provide the building blocks of the platforms for IT initiatives of the future whilst maintaining "rock solid" resilient and secure services through our cybersecurity programme. However, our technology estate remains complex and needs to continue to evolve to meet the needs of the future. Some of the key areas of focus for GD3 are:

¹ <https://www.sgn.co.uk/sites/default/files/media-entities/documents/2024-03/SGN%20Digitalisation%20Strategy%20March%202024.pdf>

² [SGN NIS Annual Report 2024](#)

SGN IT and Telecoms Strategy

- During GD2 we adopted an industry-leading “cloud-first” strategy however due to the need to disaggregate our IT from SSE and exit its datacentres this drove a “lift and shift” approach for expediency – virtualisation of physical servers into Infrastructure as a Service (IaaS) without significant transformation of the complex application estate. While necessary and appropriate to achieve our aims at the time, our intended strategy in GD3 will enable us to unlock the full benefits from a move to cloud “Platform-as-a-Service” or “Software-as-a-Service” (PaaS/SaaS) such as seamless patching and updates, increased availability, resilience and scalability.
 - The application estate has grown over time to as a result of evolving business needs to more than 200 applications. The inflexibility and cost of change of traditional “commercial off the shelf” (COTS) applications has led to the implementation of various point solutions to meet specific business requirements, which has resulted in some overlap and applications that are not as cohesively integrated as they could be, which limits the efficient flow of data across the business. Many of our applications are approaching the end of vendor support on their current versions and so require upgrades to remain supportable. Finally, there is also additional functionality that’s needed to fully digitally enable our workforce – primarily a workflow and field service management platform. There is an opportunity to consolidate functionality, simplify the application estate and improve resilience by adopting SaaS and PaaS services and a need to invest in upgrading end of support applications.
- [REDACTED]
- Our networks are secure and resilient using tried and tested Multi-Protocol Label Switching (MPLS) architecture, but as we drive into the world of cloud and Software as a Service (SaaS) applications this will become a choke point and we need to shift towards adoption of zero-trust security models with software defined networks that enable more scalable, flexible and cost-effective connectivity to continue to manage a 24/7 available telecoms network that meets the needs of the business. Leveraging the need to refresh our network infrastructure we will take the opportunity to make this evolution, deploying faster connectivity to SGN sites, increasing the use of WiFi, deploying secure, scalable VPN connectivity and increasing the resilience of our networks. Our remote sites are connected by Public Switched Telephone Network (PSTN) lines which will be switched off on 31/01/2027. This deadline, coupled with increased requirements around cyber-security mean we need to implement new, secure, resilient connectivity to a greater number of sites.
 - There are several platforms that provide integrations between platforms and applications, some of which overlap or duplicate capabilities for single business processes or systems. Our GD3 business plan includes provision to rationalise some of these into our existing Enterprise Integration platforms for performance, efficiency and reusability.
 - Our current approach for end user devices provides standard office-type laptops and commodity mobile phones to all staff including field force workers, these are cumbersome to use wearing PPE and prone to high rates of breakage in field conditions so we aim to provide more fit for purpose technology options suited to different user roles.
- 6 Looking to the future, the introduction of the National Energy Systems Operator (NESO) is likely to drive requirements for sharing data, and under the Future Systems and Network Regulations (FSNR) SGN will become a participant in and industry-wide data sharing infrastructure. It is also likely that in future there will be a requirement for automation of scenario development to support climate change resilience by sharing data with external sources such as the Met Office, the Scottish Environment Protection Agency, The Environment Agency, and other arms-length bodies, as well as universities and independent researchers. It is important to recognise that the investments contained within this area of the business plan provide the robust foundations for these future requirements (in conjunction with the investments in

data and digitalisation), but there remains uncertainty in the implementation of these measures which we would anticipate being the basis of a reopener within GD3.

Conclusions and Assurance

- 7 The investments included in the IT and Telecoms, Digitalisation and Cyber Security sections of SGN's GD3 business plan represent the digital ambition that will enable SGN to transform its capability and increase its operational effectiveness while building on our solid foundations of emergency response and customer service. The foundational investments in data and platforms will position us to confidently and automatically share more data sets supporting cross-industry alignment, supporting innovation, and driving social benefit.
- 8 In preparing these business plans we have used our own experience, and our network of IT business partners in driving an Enterprise Architecture-led approach to ensure the alignment and coherence of our bids. We have also commissioned Gartner to independently assure our costs within IT and Telecoms, Digitalisation, and Cyber Security, and they have confirmed that all our costs are realistic and within the ranges they would expect when benchmarked against their large database of reference case studies globally. We have separately submitted Gartner's assurance report in support of these business plans.

SGN IT and Telecoms Strategy

Section A Introduction

- 9 SGN's IT systems services and infrastructure underpin our ability to provide emergency response, network operations and asset management to ensure a safe and secure network, protecting life and property, to serve our customers and other stakeholders and to add social value by innovating and sharing data. This strategy complements the Data and Digitisation Strategy and Cyber Security Strategy by focussing on the following elements of the core IT landscape:
 - (a) **Networks and Telephony** – These provide the connectivity needed to enable the flow of data around, into and out the enterprise, that enable our people and partners to interact with our systems and communicate each other, and our customers to interact with our Contact Centres, whether through traditional voice telephony, messaging, or more modern collaboration services (such as Microsoft Teams). It includes traditional wide area and local area networks and the internet, wi-fi, mobile telephony as well as more specialist satellite communications for our remote sites.
 - (b) **Cloud Hosting** – SGN is one of the few utilities companies (and one of only two GDNs) that has migrated all of its IT estate on the cloud with no on-premises data centres, albeit almost entirely as Infrastructure as a Service with minimal optimisation for cloud, so this element of the strategy focusses on the way we use cloud hosting and how we optimise it to maximise business resiliency and responsiveness while minimising the cost to operate.
 - (c) **End User Compute** – This includes the devices that we issue to staff and the way we get best value from those, as well as alternatives to physical devices such as bring-your-own-device (BYOD) and virtual desktop options.
 - (d) **Integration** – These are the technologies that allow data to move between applications maintaining a consistent and coherent view of people, work and assets across the enterprise.
 - (e) **Applications** – The systems and their interfaces that SGN people, contract partners and other stakeholders use to do their day-to-day work.
- 10 These elements of our core IT landscape underpin and enable SGN to pursue the following business outcomes:

SGN IT and Telecoms Strategy

- Stakeholder and Societal Value – Underpinning our digital and data services to ensure they are inclusive, secure, sustainable and reliable. They must deliver recognisable value to our customers and stakeholders
- Regulatory Obligations – Helping to keep our people safe, ensure the safety of members of the public and protect property while operating within our legal framework of statutory law and licence conditions.
- Business Transformation – Supporting our transformation programme to rebuild our legacy business processes supported by technology, putting the IT tools in the hands of our front-line staff that best support them in their work.
- Business Excellence – IT allows us to drive performance gains in a broad range of business activity and address our most difficult problems.
- Innovation and the Future of Energy – We pilot and implement new technologies to enable performance gains in how we manage today’s network and prepare us to meet the energy demands of the future.

Purpose and Scope

Purpose

- 11 This strategy paper has been prepared as part of SGN’s submission to Ofgem to set out the context of the IT investments that SGN proposes to make to ensure the long-term sustainability, security and integrity of the services that underpin SGN’s ability to manage and maintain the gas network and assets.

Scope

- 12 This IT Investment strategy is tailored for SGN with an anticipated lifespan of about 5 years, aligning with the GD3 price control periods. While it is projected to span 5 years, the strategy will undergo annual reviews and revisions. It encompasses all IT investments plan for the GD3 price control period (i.e., 2026 - 2031), ensuring SGN’s operations is consistently supported by state-of-art technology. Notably, this is a high-level strategy with a defined lifespan. Therefore, while it provides an overview of the planned investments, it does not delve into exhaustive details for each one. Comprehensive specifics for each investment can be found in the developed Business Plan.

SGN’s Evolving Digital Landscape

- 13 The digital landscape in which our IT infrastructure operates has evolved markedly over the past few years. This evolution is driven by technological advancements, shifting business needs, new ways of working and emerging global trends. SGNs IT needs to evolve in line with these shifts to ensure it remains fit for purpose and enables us to adapt to an increasingly dynamic and changing energy landscape and remain secure and resilient to emerging disruptors.
- 14 Key factors emphasising the urgency of our IT-focused investment strategy include:
 - Increasing complexity of the cyber threat landscape: The pace of technology change and increasing geopolitical impacts to energy supplies mean that our IT systems face new and emerging threats of disruption. Ensuring that our IT systems and the gas network assets they support remain resilient and secure is not just a focus for investment in cyber tooling but requires a systematic approach throughout the whole technology stack.
 - Remote Work and Access: With a growing trend towards remote work and access to corporate resources from distributed locations, there is an intensified need to ensure reliable and secure connectivity, emphasizing robust IT infrastructure and practices. The experience of the global Covid-19 pandemic demonstrated the criticality of being able to enable our workforce to work remotely as a key resilience and business continuity measure. As half of SGN’s workforce are field-based the ability

to interact with the systems and data they need to do their jobs securely and reliably from wherever they need has never been more important.

- Legacy System Modernisation: Many of SGN’s business functions rely on IT systems that are coming towards the end of their vendor support lifecycles. These legacy systems, while often critical, may not be fully supported in the longer term, optimised for current or future business needs or support integrations with other systems, underscoring the necessity for continued upgrades and replacements to ensure they remain fit for purpose.
- Interconnectivity and Integration: As different IT systems, platforms, and applications become increasingly interconnected and the need to share and reuse data increases, the importance of ensuring smooth and secure integrations becomes paramount.
- Internet of Things (IoT): The rise of IoT devices in the corporate environment presents new challenges and opportunities. These devices, while enhancing operations, can also introduce vulnerabilities if not properly integrated and managed.
- Hybrid and Multi-cloud Environments: The move to cloud-based solutions, often spanning multiple providers, calls for a comprehensive IT strategy that addresses security, data sovereignty, latency, and interoperability and optimises software architectures to exploit the benefits of cloud.
- Supply Chain Digitalisation: As operations and supply chains become more digitally interconnected, ensuring the integrity and reliability of these digital channels becomes crucial.
- Emerging Technologies: Technologies like edge computing, artificial intelligence, and 5G are reshaping the IT landscape and offer significant opportunities for enhancing the way in which SGN manages its network and assets. Adapting to and leveraging these technologies requires foresight and strategic investment.

SGN’s GD2 Technology Transformation

- 15 Over the last four years, SGN has undertaken a major IT transformation. Our primary driver is always to provide stable and reliable technology services that protect our people and our customers. Our goals of this transformation have been to: Improve resilience and availability, improved security, increased agility, reduced costs and align to innovation and new ways of working.
- 16 We have invested significantly in technology, processes, and people to provide the building blocks of the platforms for IT initiatives of the future whilst maintaining “rock solid” resilient and secure services through our cybersecurity programme.
- 17 This work has rebuilt our IT architecture and amongst many other things, has delivered:
 - An increased and enhanced communication network using MPLS with secure cloud connectivity.
 - A new integration platform utilising API (application programming interface) architecture, brokerage, and message bus capabilities.
 - A complete migration of our core IT application estate, to highly scalable, secure, resilient, and highly available public cloud infrastructure [REDACTED]
 - We have evolved our management of the applications by introducing some elements of automation in infrastructure and application delivery and our maintenance processes by using Continuous Integration / Continuous Delivery (CI/CD) pipelines.
 - We have also recently created an organisation data lake with several use cases delivered to date.
 - A physical and technical separation from our shared network and IT infrastructure with our previous part-parent company, SSE. This activity alone has significantly reduced our Cyber security attack surface.

SGN's GD3 Investment Plans

- 18 SGN intends to build upon the foundational work delivered in GD2 to transform, consolidate and rationalise our estate in GD3, while investing in digitalisation and consolidating the progress we have made in reducing our cyber risk and achieving cyber compliance.
- 19 Because of the close linkages between core IT strategy, the digitalisation, and the cyber security, this strategy should be read alongside the SGN published Digitalisation Strategy³ and the Network Information Systems Annual Report⁴ cyber assessment submitted as part of these business plans. The Digitalisation Strategy describes investment in data and digitalisation as a means to drive social benefit, regulatory compliance, business transformation, business efficiency and innovation. These two areas of our business plan are closely integrated as well as being managed as a single portfolio of investment and therefore in this section we will outline the investments in both of these areas. This portfolio is also closely linked to our Cybersecurity portfolio and hence Table 1 below shows summary values for all three business plan areas.

Table 1 - IT, Cyber, and Digitalisation investments in the SGN GD3 business plan

	26/27 (£m)	27/28 (£m)	28/29 (£m)	29/30 (£m)	30/31 (£m)	Total (£m)
Ongoing Maintain and Run:						
IT Opex Ongoing Costs	39.2	39.2	39.5	40.0	40.3	198.2
Investment Costs						
IT and Telecoms Group Capex	21.5	38.7	33.5	16.5	5.1	115.2
IT Opex Projects	1.8	3.1	1.8	0.8	0.9	8.4
IT Opex Projects Ongoing Opex	1.3	1.4	1.4	1.5	1.5	7.0
Cyber Security						
Cyber Capex	22.1	11.6	7.7	3.3	3.6	48.5
Cyber Opex	24.6	25.5	25.2	24.6	24.7	124.6
Data and Digitalisation						
Data and Digitalisation Capex Projects	2.4	2.4	3.0	2.1	2.2	12.0
Data and Digitalisation Opex Projects	2.0	2.1	1.8	0.6	0.2	6.6
Data and Digitalisation Ongoing Opex	1.1	1.3	1.2	2.3	2.2	8.2
Total IT and Telecoms Group	115.9	125.3	115.1	91.7	80.7	528.7

Source: SGN

- 20 Our approach to ongoing "Run" IT Opex has been to trade off consolidation and decommissioning benefits driven by investment with the need to absorb new applications and platform operating costs, as well as absorb inflation and general upward cost pressure as long-term pricing deals with suppliers expire. Where we are introducing a new system that replaces an existing system, we have treated this as a like-for-like replacement in our calculation of Opex and signalled only the delta between the old system and the new system in our project ongoing opex numbers.
- 21 In summary, as can be seen from the table, running SGN's current IT and Telecoms estate is projected to be a flat rate of c £40m per annum, with the delta introduced by new technology platforms (netted off

³ <https://www.sgn.co.uk/sites/default/files/media-entities/documents/2024-03/SGN%20Digitalisation%20Strategy%20March%202024.pdf>

⁴ SGN NIS Annual Report 2024

SGN IT and Telecoms Strategy

against the platforms they replace) adding approximately £1.5m per annum. On that same estate the introduction of new digitalisation assets will add £1.2m per annum in the first year of GD3, progressively rising to £2.2m by the last year as new assets are introduced. Although cyber investments and their associated run costs are dealt with in the separate cyber strategy, CBAs and EJPs, it should be noted that investment in cyber assets over GD2 and in reopeners has led to a requirement for cyber operating costs of c. £25m per annum throughout the GD3 planning period.

IT and Telecoms Initiatives

22 Table 2 shows the costs of the IT and Telecoms initiatives described in strategic terms within this paper which are broken down in detail in the associated Engineering Justification Papers and Cost-Benefit Analyses referenced in the table.

Table 2 - IT and Telecoms Initiatives contained in the SGN GD3 Business Plan

Table with 6 columns: Initiative, Project Capex (£m), Project Opex (£m), Ongoing Opex (£m), Total (£m), and Doc Refs. Rows include Field Service Replacement, Enterprise Asset Management (EAM), Enterprise Resource Planning (ERP), Specialist Applications, Integration Services, Hardware Devices, Software Platforms, Data and Telecoms Refresh, Mandatory IT System Change, and Learning and Competency Management.

Xoserve	■	■	■	■	
Customer and Stakeholder	■	■	■	■	
Total IT and Telecoms Core-IT Initiatives	115.2	8.4	7.0	130.7	

Source: SGN

Data and Digitalisation Initiatives

- 23 Because the SGN Digitalisation Strategy is a separately published document and not a specific deliverable for the GD3 business plan, and also because the IT and digital estates are part of the same coherent estate to operate, we have included a summary of the data and digitalisation initiatives below in Table 3. Business cases and justification papers have been provided for each initiative as referenced.
- 24 Against the 11 principles of Data Best Practice Guidance (DBPG) SGN is currently compliant with 9 principles (as they are currently defined) and have plans in place to achieve compliance with the remaining two within the GD2 period. Some examples of action we have taken to comply with these principles include:
 - The publication of 6 open data sets (with two more under development) on SGN’s open data portal, alongside a public data catalogue to ensure data assets are discoverable.
 - The adoption of Dublin Core as an industry-standard metadata approach, and the publication of metadata alongside our published open data sets, which provides supporting information to enable potential data users to understand the data assets.
 - SGN’s annual stakeholder engagement plans have been used to understand the needs of current and prospective data users and these have been included in the published Digitalisation Strategy. Further developments of this will include enabling data consumers to access data through APIs to automate data access.
 - The consistent application of SGN’s Cyber security framework to all data products and services which are in accordance with security privacy and resilience best practices
 - SGN is a member of the Gas Data Collaboration Group (GDCG) which has been established to coordinate data sharing efforts across the GDNs. Through this group we have created an initial set of data assets that have common definitions and formats with other gas networks. In lieu of specific technical standards being defined by the data sharing infrastructure, we have aligned with open source standards.
- 25 Continued good performance against DBPG is predicated on continued collaboration and co-development of standards and guardrails across the industry, and is also predicated on the investments detailed in our Data and Digitalisation GD3 plans. We recognise that DBPG continues to evolve and hence continued funding will be needed to deliver during GD3, with the backdrop of FSNR and the data sharing infrastructure.
- 26 Our detailed plans and framework for DBPG are contained and encapsulated within our Digitalisation Strategy which we intend to republish in Q1 of the financial year 2025-26 taking into account Ofgem’s feedback on our GD3 business plan, so that we are able to coordinate and align strategy with funded business plans.

Table 3 - Data and Digitalisation Initiatives contained in the SGN GD3 Business Plan

Initiative	Project Capex (£m)	Project Opex (£m)	Ongoing Opex (£m)	Total (£m)	Doc refs
Catalogue and Master Data Management	■	■	■	■	■
Data Governance	■	■	■	■	■
Recruitment Apprenticeships and Data Literacy	■	■	■	■	■
Data Platform and Model	■	■	■	■	■
Business Analytics and Exploration	■	■	■	■	■
Total Data and Digitalisation Initiatives	12.0	6.6	8.2	26.8	

Source: SGN

Cyber Security Initiatives

27 Because the SGN Cyber assessment and action plan is a separate deliverable and is not a specific part of the GD3 business plan submission, we have included a summary of the cyber initiatives in Table 4. Business cases and justification papers have been provided for each initiative as referenced.

Table 4 - Cyber Security Initiatives included in the SGN GD3 Business Plan

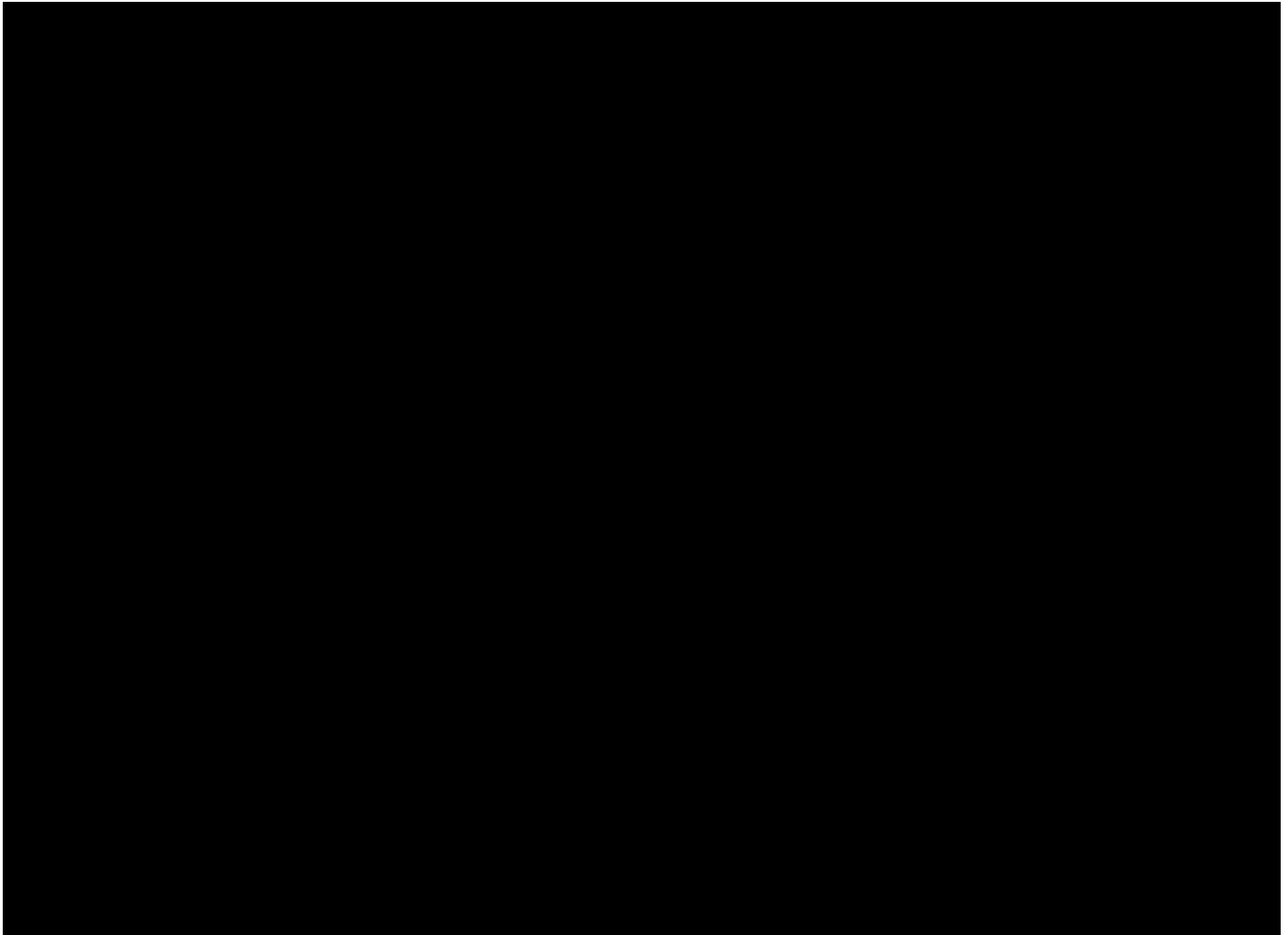
Cyber Initiatives	Project Capex	Project Opex	Total	
■				
■	■	■	■	■
■	■	■	■	
■	■	■	■	
■	■	■	■	
■	■	■	■	
■	■	■	■	
■				
■	■	■	■	■
■	■	■	■	

SGN IT and Telecoms Strategy

[REDACTED]	■	■	■	[REDACTED]
[REDACTED]	■	■	■	[REDACTED]
[REDACTED]	■	■	■	[REDACTED]
[REDACTED]	■	■	■	[REDACTED]
[REDACTED]	■	■	■	[REDACTED]
[REDACTED]	■	■	■	[REDACTED]
[REDACTED]	■	■	■	[REDACTED]
[REDACTED]	■	■	■	[REDACTED]
[REDACTED]	■	■	■	[REDACTED]
Total Cyber Initiatives	48.5	124.6	173.0	[REDACTED]

Source: SGN

The SGN Estate

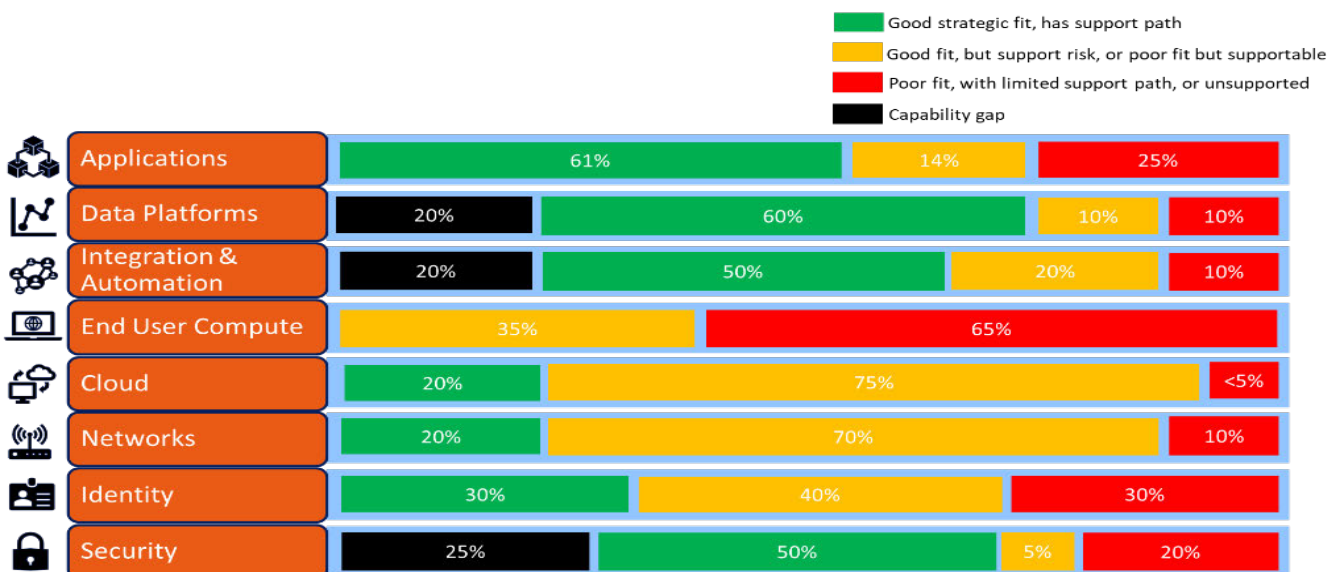


- 28 Figure 1 shows a rich-picture overview of the SGN IT estate. Much progress has been made during GD2 including the move from SSE owned data centres to the cloud, adoption of modern workplace tools, added resiliency of our networks and significant investments in cyber security. However our technology estate remains complex and needs to continue to evolve to meet the needs of the future. Some of the key areas of focus for GD3 are:
- (a) Our cloud transformation programme and “cloud first” strategy accompanied latterly with the need to disaggregate our IT estate from SSE and exit its datacentres during GD2 drove a “lift and shift” approach to cloud migration which was the most effective and efficient mechanism to achieve customer benefits at that time. Having moved our application and platform estate into AWS cloud hosting, in the majority of cases this has been achieved by using infrastructure-as-a-service (IaaS). This means that physical servers in datacentres have been replaced by virtual ones in the cloud, but the operating systems, middleware and applications that sit on those servers remain the same. This move has benefitted our ability to size our server estate to the needs of our applications without having to procure and manage physical hardware assets, and has also reduced the risk of application outage caused by physical hardware failure, as well as significantly better security, but we are not yet gaining the benefits that could be achieved with software-as-a-service (SaaS) including patching and vulnerability management being the responsibility of the vendor, and new features and updates being available to users without a lengthy regression testing and release process. Our GD3 plans build logically on the firm foundations of moving to the cloud in GD2 by driving the shift to SaaS platforms to achieve these further benefits.

SGN IT and Telecoms Strategy

- (b) The application estate has grown over time to as a result of evolving business needs more than 200 applications. The inflexibility and cost of change of traditional “commercial off the shelf” (COTS) applications has led to the implementation of various point solutions to meet specific business requirements, which have overlap and are not cohesively integrated, which limits the efficient flow of data across the business. Many of our applications are approaching the end of vendor support on their current versions and so require upgrades to remain supportable. Finally there is also additional functionality that’s needed to fully digitally enable our workforce – primarily a workflow and field service management platform. There is an opportunity to consolidate functionality, simplify the application estate and improve resilience by adopting SaaS and PaaS services by which we can improve user satisfaction and productivity while reducing cost, complexity and reduce the risk of operational failure. This also reduces the risk of cyber-attack by presenting a smaller attack surface.
- (c) Our networks are secure and resilient using tried and tested Multi-Protocol Label Switching (MPLS) architecture. In the past this has been the right choice for SGN because of its reliability, scalability and security by virtue of it being a private network partitioned off from the public internet. Designed around our current applications strategy with the bulk of our applications in IaaS within a single cloud provider this network topology makes sense. But as we drive further towards SaaS applications the hub-and-spoke model for networks increasingly becomes a choke point and it is more efficient and less expensive to connect distributed sites directly to the internet to access SaaS services. Therefore our network journey in GD3 will see us adopting software defined networks (SDNs or SD-WANs) with a zero-trust security model.
- (d) We exchange data with a number of third parties through point integrations which need to be individually maintained, secured and updated. In GD3 we will seek to consolidate around a few integration technologies that are more agile, resilient and secure than point integrations and enable reuse where multiple users or systems need access to the same data sources.
- (e) Front line staff have the same laptops and mobile devices as office-based staff which are not ideally suited for the environment in which they are used (within vans and on-site) leading to higher failure rates than those in offices. In GD3 we will address this by providing higher specification, toughened devices for front line staff.
- (f) Our remote sites are connected by Public Switched Telephone Network (PSTN) lines which will be switched off on 31/01/2027. This deadline, coupled with increased requirements around cyber-security mean we need to implement new, secure, resilient connectivity to a greater number of sites.






Figure 2 - Obsolescence in the current SGN IT Estate



Source: SGN

29 Figure 2 shows the current level of obsolescence in the SGN estate. This demonstrates that while there are areas of strength, there are also missing capabilities highlighted by the black bars, areas indicated in red where we already have risk associated with obsolescence, and areas indicated in yellow where either we have a supportable current technology that will not meet the future needs of the business, or our current technology has a degree of risk around its future supportability – i.e. the manufacturer has declared an end-of-life date that is driving us to change. The current levels of obsolescence despite previous investments reflect the fact that IT assets have a finite lifecycle and need ongoing investment to maintain them in an operable and supportable state. New and emerging threats and demands stretch the needs for our IT estate beyond their current capabilities necessitating continuous change and adaptation. The impacts of these factors across the different technology domains in our IT estate is not linear, meaning that some domains have more significant requirements for investment than others. Moreover this view is a snapshot of the current situation. Lack of ongoing investment in areas that are currently in support will lead to their deterioration over time.

Figure 3 – Investment themes by domain

	Applications	Move towards a SaaS-first/Platform architecture retaining IaaS and bespoke applications only where it is essential to highly configure or differentiate from mass market products. Deliver a reliable and consistent user experience optimised for the device they're working on.
	Data	Continue to develop and improve our platforms and capabilities to support improved data governance and quality, enable data sharing and exploit data analytics and reporting capabilities to drive better business insights. Explore the use of emerging, innovative technologies (ie Artificial Intelligence/Machine Learning, Digital Twins) where these offer viable opportunities.
	Integration & Automation	Consolidate on and support core integration capabilities and platforms that enable interoperability between systems and the right data to be surfaced to the right place at the right time, consistently, reliably and securely. Automate processes and workflows where feasible to minimise risk of error and increase data quality.
	End User Compute	Cloud based control and management of all devices allowing for a move to zero trust. Enable quick and simple set up of SGN and contract users from any network location on any device. Continue to Exploit our MS licensed products to drive value from that investment. Provide users with the appropriate device for their role (ruggedised/mobile devices for field workers, BYOD/Virtual Desktop options) .
	Cloud	Adopt best practices to optimise and manage our cloud footprint such as the use of native services and containerisation, Infrastructure as Code, DevOps. Continue to improve and integrate our monitoring capabilities.
	Networks	Break our dependency on legacy MPLS, traditional VPNs and external core network. Focus on enabling a secure zero trust, efficient, low cost, flexible set of connectivity solutions that enable users to access the services and data they need from wherever they need to work.
	Identity	Fully establish HR data as the master source of identity and maximise the use of cloud identity platforms with a long-term view to discontinue our use of traditional on-premises (IaaS) MS Active Directory and enable the move to a zero-trust security posture.
	Security	Deliver the capabilities needed to support the move towards zero-trust, cloud and SaaS-based services and "work anywhere". Prepare for new and emerging cyber challenges such as Quantum and AI ubiquity.
	Operational Technology	Deliver enhancements to our Operational Technologies that improve the security and supportability, enable better insight and control of and future-proof our critical Gas Control assets in order to sustainably deliver the future energy needs of our customers.

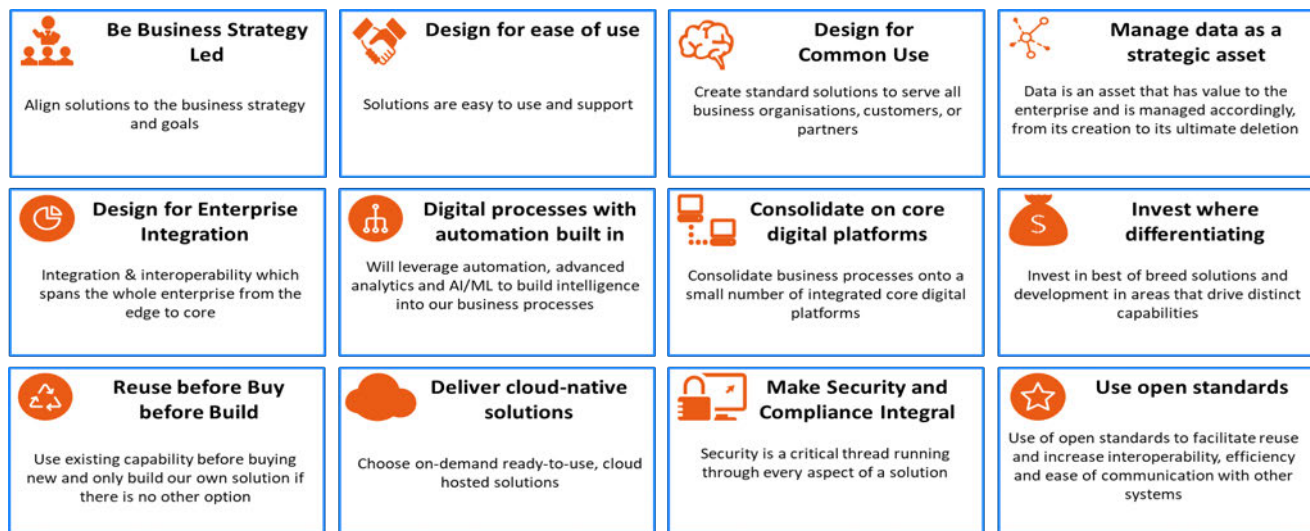
Source: SGN

30 Using the analysis of our estate in Figure 2, Figure 3 shows the main investment objectives for each domain. Note that for completeness we have also included security and data as domains in this view, but these are the subject of their own strategies which are complementary to this one.

Enterprise Architecture-led Approach and Assessment Processes

- 31 Throughout the development of our IT and Telecoms Strategy and GD3 technology investment priorities we have taken a holistic, Enterprise Architecture-led approach, developing overarching roadmaps across our key technology domains. These have been developed in line with our Enterprise Architecture Principles and guardrails, taking into account technology industry best-practices and trends in context of SGN’s business strategy and goals. This has enabled us to assess the investment options for fit to regulatory obligations, policies and business outcomes and ensuring technical alignment across domains so that we have confidence in the deliverability and long-term sustainability of our IT estate.
- 32 Figure 4 shows SGN’s Enterprise Architecture Principles which have been used as a high-level guardrail for our technology choices. The detailed rationale for technology decisions in each investment area is set out in the related EJPs.

Figure 4 – SGN’s Enterprise Architecture Principles



Source: SGN

Section B Networks and Telephony

Overview


- 33 SGN’s current enterprise network was designed primarily around a central core network to support SGN cloud hosted front / back-office applications during the migration away from physical data centres in 2019. While this design was suitable at the time, SGN are now using more 3rd party hosted SaaS applications, has more remote working users and has adopted collaboration tools across the userbase for voice and data sharing.
- 34 Refreshing the network in a timely cycle avoids SGN operating with non-performant and potentially vulnerable connectivity, which in turn would result in the staff being unable to perform their duties, ultimately impacting on safety to both them and the public, and impact to licence obligations.
- 35 The ability to maintain an operational communications network that enables our staff to access and share data to undertake their work effectively on 24x7 basis is critical to our successful delivery of our regulatory and customer service obligations. The investment planned in GD3 will support the modernisation and resilience of our networks to ensure that they can support our workforce into the future.

SGN’s Objectives for GD3

- 36 **In GD3 SGN must deploy new, faster site connectivity to all corporate SGN locations to meet increasing bandwidth demands.** SGN has established corporate voice and call center using MS Teams and is heavily reliant on productivity collaboration tools across the user base resulting in considerable network traffic increase. To keep pace with the demand created by higher bandwidth applications and tools, all SGN locations must be upgraded to a faster network connection. As part of this change, we will migrate where possible away from existing MPLS links to fast direct internet services with edge security.
- 37 **Increase use of WIFI across the estate.** This will reduce reliance on costly network switching equipment and associated cabling and increase flexibility. Wi-Fi demand has grown significantly throughout the GD2 period. Wi-Fi in SGN is not currently centrally managed, often has limited coverage and many sites have limited bandwidth which is not meeting user expectations.
- 38 **Deploy secure scalable enhanced VPN network connectivity.** This will focus on ease of use, performance and in preparation for ZTNA (Zero Trust Network Architecture). SGN has a significantly increased number

of remote working users following the pandemic. In 2019 remote workers consumed approximately 700 concurrent VPN connections, in 2024 this has risen to 3000 concurrent connections on any business day.

- 39 **Increase network resilience by removal of single points of failure across the network estate.** This will identify and remove traffic pinch points and single points of failure across the SGN network and improve high availability network capabilities.

40 

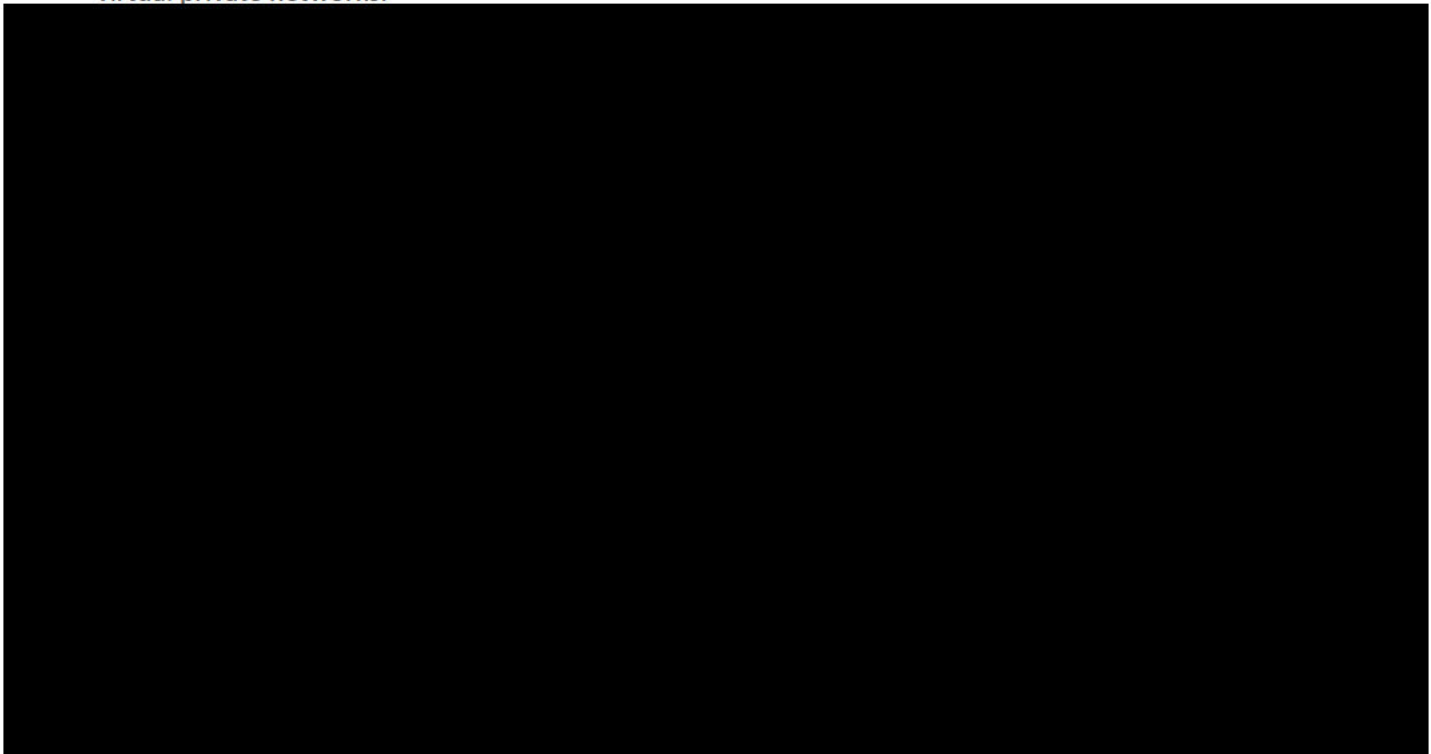
- 41 **Enhanced proactive network monitoring.** This will increase proactive monitoring capability across the estate, incorporate firewalling and VPN services. Integration with SGN's Security Operations Centre service is required for critical security event management.

- 42 **Refresh of corporate voice telephony and call centre services.** This will include refreshing call centre voice solutions in the Operational Control Centre (OCC), Customer Experience, and Gas Control. These will require a modern unified solution that facilitates flexible and remote working. We must also refresh the existing current voice-over-internet-protocol (VOIP) solution to incorporate new features and simplified management. For cellular based communications, we will enhance use of roaming capabilities from mobile providers to assist coverage in remote areas.

- 43 **Refresh the training sites communications and infrastructure.** Our training facilities are experimenting with the latest digital training tools including augmented reality and immersive technology as well as the more traditional e-learning and classroom-based training. This digital shift will need the addition of higher bandwidth network services.

GD3 Roadmap

- 44 Figure 5 shows the current state network topology with most of our application estate hosted on AWS, which is connected to our corporate MPLS network which use internet gateways to enable access through virtual private networks.



Source: SGN

- 45 SGN's desired target state is to adopt a secure access service edge (SASE) model which will be better aligned to our future business need. Anticipated benefits include greater resilience and stability reducing network downtime, enhanced cyber security and compliance with the enhanced cyber assessment framework (E-CAF), higher bandwidth with reduced latency driving a better user experience, and reduced costs to operate and maintain the network.
- 46 The roadmap to achieve this contains two main items:
- **Decentralisation of internet access to sites.** This is achieved by delivering internet connectivity direct to each site rather than through the MPLS. This removes the MPLS network as a pinch point and enables network security to be managed by local security appliances with secure VPN tunnelling to access business applications [REDACTED]
 - **Movement to Secure Access Service Edge (SASE) model.** This will be achieved by removing the SGN hosted gateways and moving to a SASE provider to run VPN connectivity as a service with onward service connections to the SGN network and cloud estate.
- [REDACTED]

Section C End User Compute

Overview

- 47 End User Compute encompasses the devices that our workforce use – desktops, laptops and mobile, which enable them to access the applications and data they need to do their jobs, whether that be in an office environment, or in the field, and the technology and tooling needed to manage and secure those devices. [REDACTED]

SGNs Objectives for GD3

- 48 Our strategy for End User devices (such as laptops, tablet devices and mobile phones) is based on a vision of delivering a reliable, secure and appropriate device into the hands of our users that is best suited to

enable them to fulfil their particular role. Core to that is understanding the different user needs throughout our workforce, from our Front-Line operatives who need rugged, and intuitive devices to use in the field, through to our staff in supporting teams who need a more standard device that enables them to use productivity software and back-office applications to enable them to do their jobs efficiently and effectively.

GD3 Roadmap

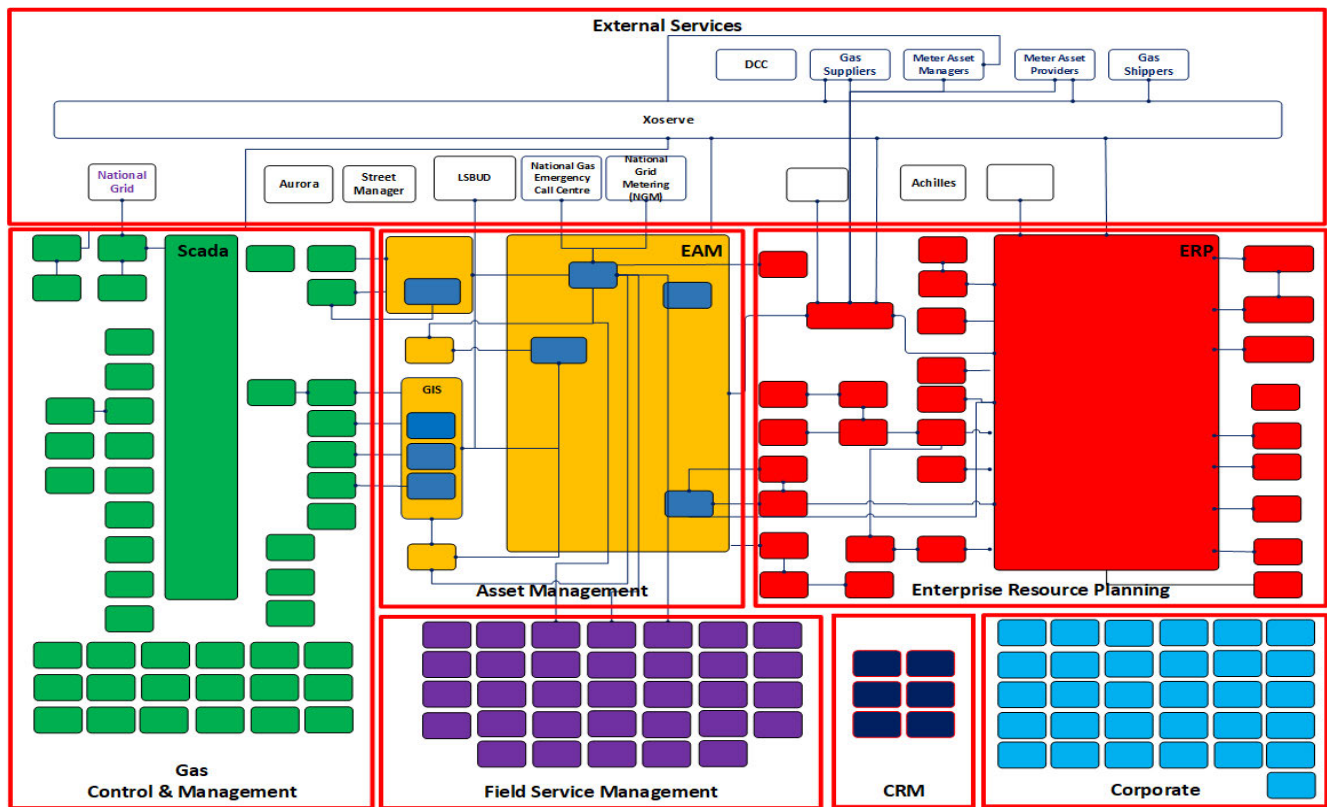
- 49 The roadmap to get there is intrinsically linked to other aspects of our technology estate modernisation, from ensuring that the tools and applications used by our Front-Line workers are mobile ready and ensuring that our users have the connectivity to access the data and systems they need to do their job whether they be in the office, working at home or in the field. Therefore, device refresh cycles early in the GD3 period will focus on bringing our devices up to a baseline specification that will meet the demands of our software and applications moving forwards and giving our field staff ruggedised devices to minimise breakages. Subsequent investment cycles later in GD3 are expected to support the rollout of higher specification mobile Android or iOS devices to front-line staff to enable a more intuitive interaction with our modernised applications.
- 50 Use of “Bring Your Own Device” (BYOD) and provisioning of virtual desktops will support a more flexible approach to providing authorised access for our data and systems for our approved third-party suppliers and partners.
- 51 A move towards a modern cloud-based approach to device, application and access management capabilities will help enable more efficient provisioning, monitoring and management of user devices which, along with robust identity management and security tools supporting a “zero trust” (we assume that users and devices are untrusted and so must be authenticated) and “least privilege” (users and devices are only given the minimum privileges needed to fulfil their role) approach will ensure that our data and critical systems remain secure regardless of where they are being used and by who.
- 52 While in general we aim to minimise our reliance on paper and printing through digitisation of processes as part of our application modernisation there are still some remaining requirements for physical printing, such as generation of customer letters or for Business Continuity Measures. We intend to implement improvements in the centralised management and monitoring our remaining printer estate to ensure its reliability and availability when needed.

Section D Applications and Cloud

Overview

- 53 SGN’s applications estate number approximately 200 business applications – which against all benchmarks for the size, scale, and type of business is high. The application estate has evolved over time in response to evolving customer and business needs which has led to some overlapping of technologies and point solutions. The relative complexity of these different platforms means that the cost of change is high compared with a simplified estate. [REDACTED]

Figure 7 – The SGN Applications Landscape (Illustrative of key application domains and number of applications)



Source: SGN

54 Figure 7 shows the current SGN applications landscape organised by applications domain. Although there is a lot of complexity the landscape falls broadly into the following sections:

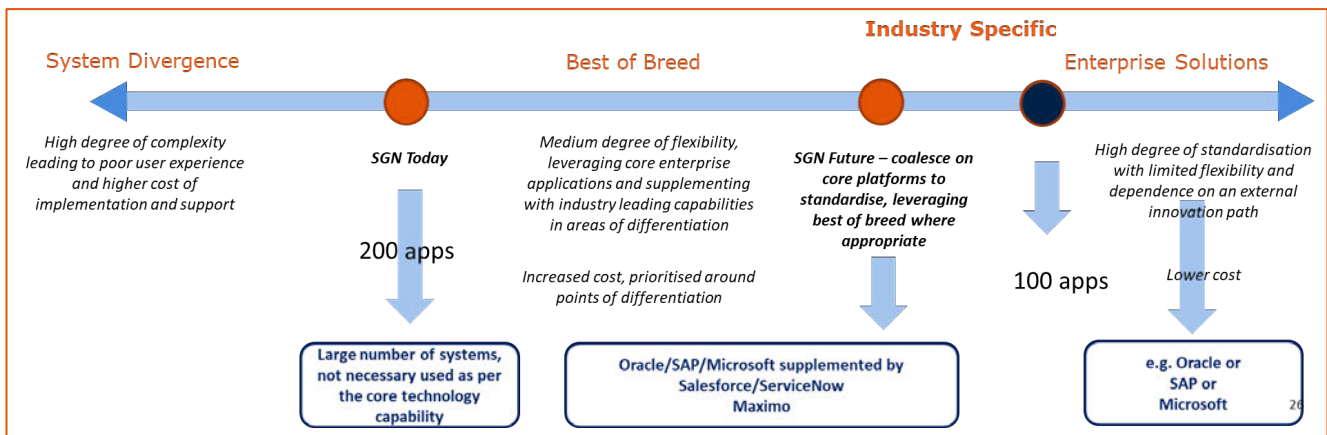
- (a) Gas Control – At the core of this is SCADA and although there are occasional overlaps between this domain and the others, it has been isolated as far as possible [REDACTED]
- (b) Asset management [REDACTED]
- (c) ERP and Billing [REDACTED]
- (d) Field Service Management – a range of applications used by field workers to access and record data related to the tasks they carry out. Shown in purple.
- (e) CRM [REDACTED]
- (f) Corporate – Other applications that support the running of SGN’s business. Shown in blue

55 With market and technology advances, there is now an opportunity for improved, automated integration between individual applications which means that currently, front line staff often have to re-key the same information into different applications which leads to low user satisfaction because of the number of systems needed to complete standard processes. This also means that there is lower confidence in the data captured in core systems and that management reports are in many cases manually compiled from a variety of sources and hence subject to additional checks and balances to ensure correct.

- 56 One capability that can be better developed in GD3 is automated “workflow” – the ability for staff to digitally follow standard processes within their application platforms, where people have a personalised list of what they are working on now and next, and customer and/or managers can track who is assigned to what work. This missing capability has been filled locally in depots by a variety of manual and shadow IT solutions that are collectively inefficient and manually intensive.
- 57 SGN lacks capabilities around HR self-service, shift and absence management for example which make the management of resources significantly more manual and onerous than it could be if we modernised our approach and systems around Enterprise Resource Planning (ERP). Our wider business plan is predicated and dependent upon the efficiency gains brought about by delivering this technology.

SGN’s Objectives for GD3

Figure 8 – SGN Platform Strategy Continuum

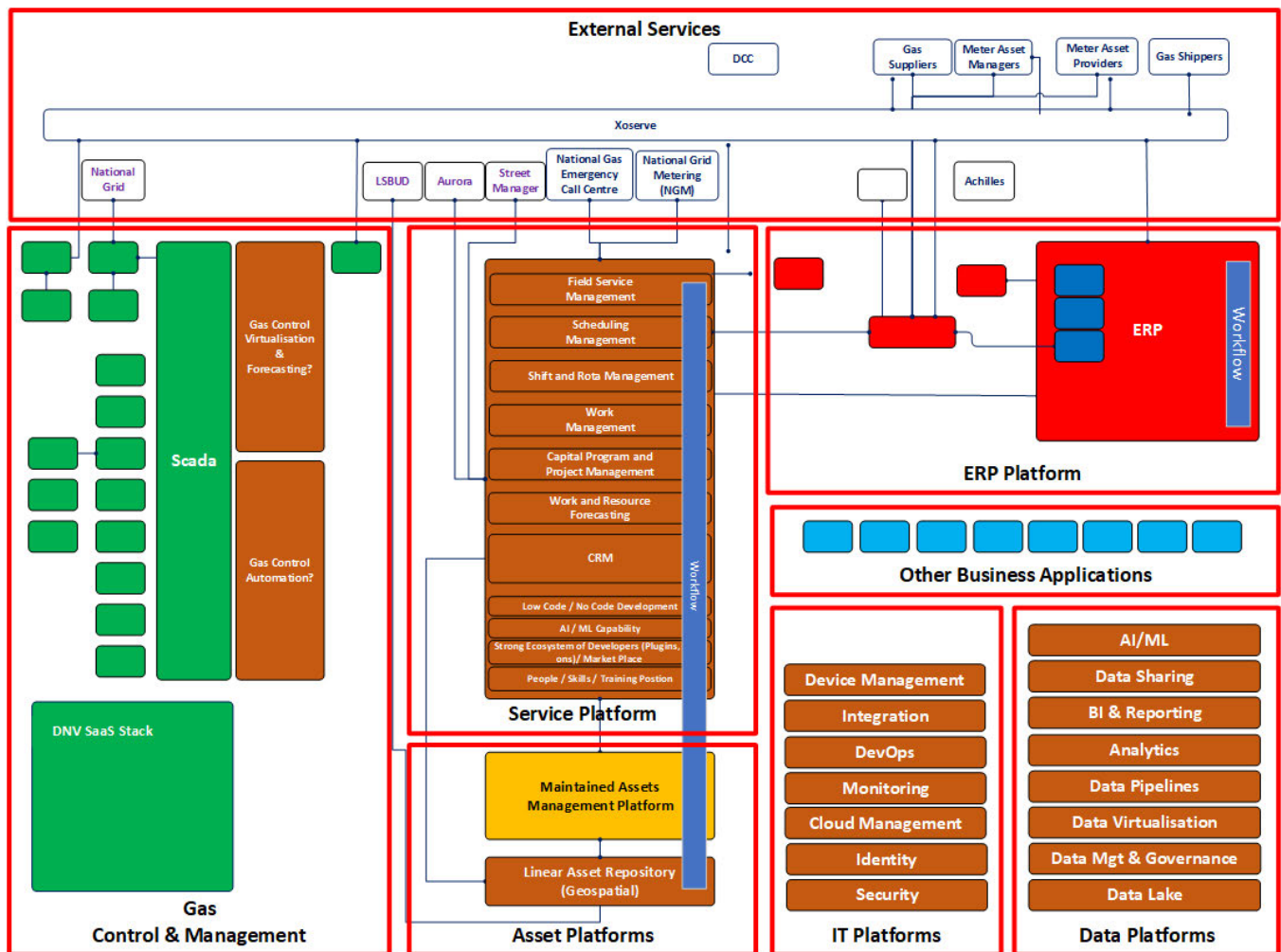


Source: SGN

58 As described by SGN’s enterprise architecture principles, the applications estate is driving towards a future of consolidation and movement to cloud SaaS services. One strategic consideration was the degree of consolidation to target. Figure 8 shows a continuum from SGN’s current state with a high degree of divergence and overlap, customisation and critical gaps, to two possible future states. In the first, SGN consolidates on a few best-of-breed SaaS platforms and uses these to remove about 100 applications from its estate. In the second SGN moves to a single platform such as SAP or Oracle which consolidates the applications estate further, reducing integration complexity and bringing down support costs.

59 SGN has elected to adopt a best-of-breed strategy. [REDACTED] The advantages of this over a single platform are that it is an easier route to adoption because it is an iteration of the platforms we already have and retains a high degree of agility and flexibility. Adopting a single platform strategy would have been the lowest cost of ownership over a 10-year horizon and would drive towards further efficiency and integration but would have a much higher cost to change and would place additional change-load on staff and higher risk of service failure and customer impact. The GD3 business plan reflects the best of breed option, which is the lowest cost within GD3 and retains a high degree of business agility.

Figure 9 - A Best of Breed Future Landscape

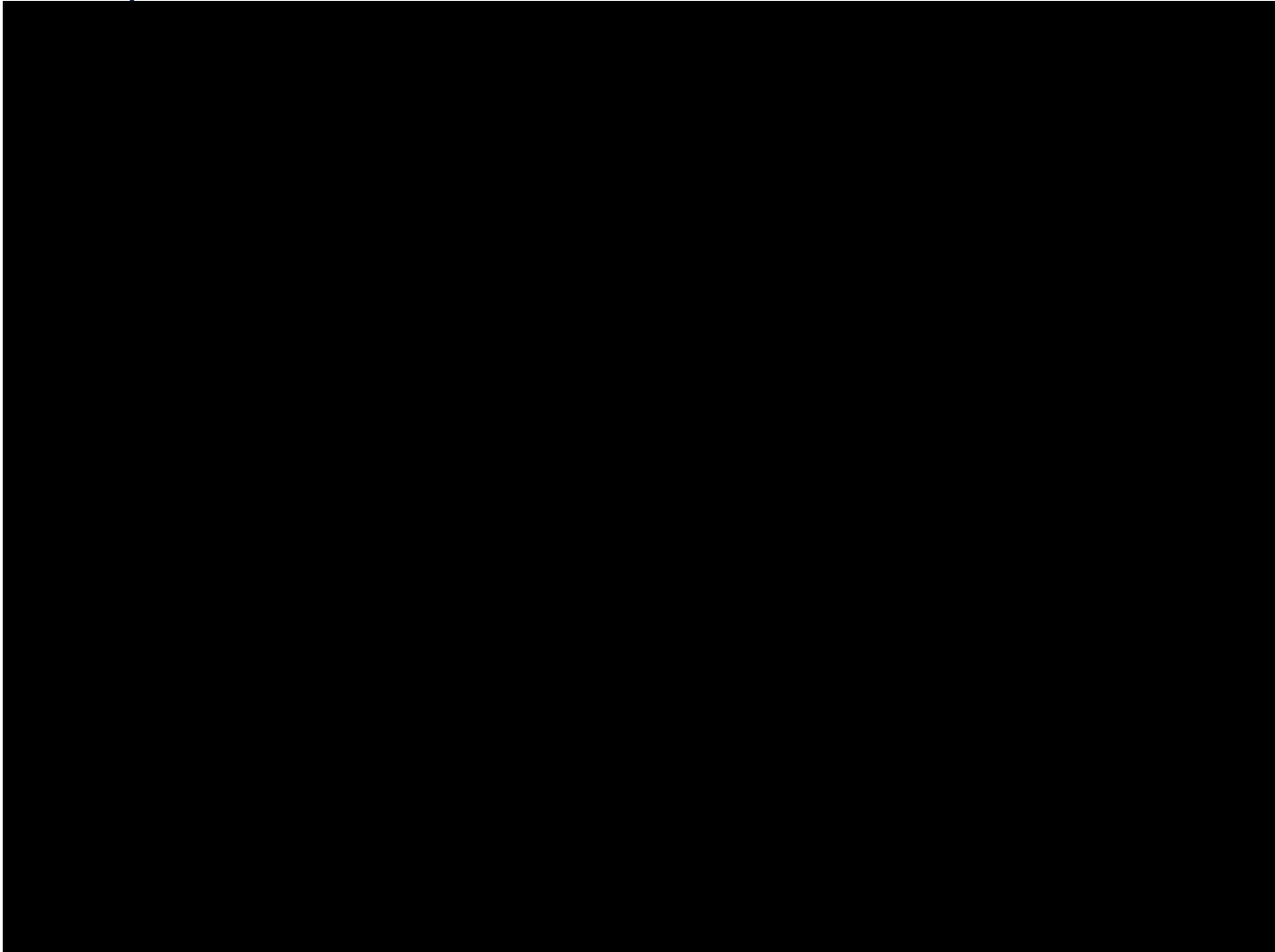


Source: SGN

- 60 Figure 9 shows a revised and consolidated landscape where elements of the extended platform ecosystems are aligned with the consolidated platforms, showing the level of convergence that may be expected from adopting a best-of-breed consolidation strategy.
- 61 The introduction and implementation of a core Field Service, CRM and Workflow platform allows us to consolidate multiple legacy applications and fill existing gaps in our capabilities to provide a single coherent, configurable and scalable Software as a Service platform that enables the creation, scheduling and management of work for our Front-Line staff, surfaced through a simplified and intuitive digital field service mobile interface. This will enable the simplification and removal of customisation in our core enterprise asset management platform, along with an upgrade and consolidation geospatial systems which, integrated with the field service platform will provide a seamless and efficient process for the management of our assets in the field.
- 62 Migration of our enterprise resource planning platform to a modern cloud SaaS service will enable us to fully exploit the capabilities of that platform to streamline, automate and future-proof our core back-office processes around finance, human resource management, procurement and logistics to ensure that we have the right people and materials available at the front line.
- 63 The implementation of more coherent and mature capabilities for the management, sharing, analysis and visualisation of our data will enable greater insight and open the opportunities to exploit technologies such as Artificial Intelligence and Machine Learning to drive greater efficiency and deliver an improved service for our customers.

- 64 Following on from the successful migration of our Gas Control systems to the AWS cloud we will continue to invest in upgrading and maintaining our core SCADA systems and explore how new and emerging technologies can enable better forecasting, monitoring and management of the gas network.
- 65 Underpinning all of this, the consolidation of supporting IT platforms to provide effective management, monitoring and visibility across our technology estate will enable us to ensure the security, availability and integrity of our data and systems.

Roadmap for GD3



- 66 Figure 10 shows a high-level view of major platform consolidation and movement to SaaS over the GD2 to GD4 timescales. In the following paragraphs we describe the scale of work that is included in our GD3 business plan within the context of this overall roadmap.

Field Service (including CRM, Work Management, Scheduling, Mobile and Workflow)

- 67 Our GD3 business plan includes investment to establish a New Field-force, workflow, mobile, CRM and scheduling Platform which will:

- [Redacted]
- [Redacted]
- [Redacted]

SGN IT and Telecoms Strategy

- Deliver Workflow, currently a missing capability which underpins and enables the automation and digitisation of all business processes
- Decommission a number of smaller applications which are point solutions used in the field, driving towards a consistent and coherent user interface (a “single pane of glass”)

68 Further details of the rationale for this approach are contained in the relevant EJP & CBA documents⁵.

Asset Management

69 [Redacted]

70 [Redacted]

Further details of the rationale for this approach are contained in the relevant EJP & CBA documents⁶

Enterprise Resource Planning

71 [Redacted]

Further details of the rationale for this approach are contained in the relevant EJP & CBA documents⁷

Integration Platforms

72 These are technologies that provide integrations between business platforms and applications, some of which overlap or duplicate capabilities for single business processes or systems. There is an opportunity to rationalise some of these into our existing Enterprise Integration platforms. Regular maintenance on these is required to maintain them in support during GD3, this includes:

- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]
- [Redacted]

Maintenance of SGN’s Cloud Estate

73 The SGN IaaS estate on [Redacted] needs to be maintained throughout GD3 as we progressively move towards SaaS.

Software Upgrades

74 This includes keeping the lights on upgrades to our client, server, operating system and middleware estate. Moving to SaaS will reduce the volume and cost of the server side changes in future. Also required is monitoring enhancements to meet minimum regulatory requirements, [Redacted]

75 [Redacted]

IT Asset Management

76 We will assess the current mobile device management solution and identify areas which are inefficient or insecure. Implement enough enhancements to achieve a more reliable solution that meets the minimum requirements. The mobile device management element of this in particular is needed to support the field services replacement and associated device strategy.

Section E Conclusions and Assurance

77 We are confident that the investments included in the IT and Telecoms, Digitalisation and Cyber Security sections of SGN’s GD3 business plan represent the level of digital ambition that will enable SGN to transform its capability and increase its operational effectiveness while building on our solid foundations of emergency response and customer service. The foundational investments in data and platforms will position us to confidently and automatically share more data sets supporting cross-industry alignment, supporting innovation, and driving social benefit.

78 In preparing these business plans we have used our experience of doing similar work before, and our network of IT business partners including Deloitte, IBM, and CGI to develop realistic costs linked to robust and deliverable implementation plans using an Enterprise Architecture-led approach to ensure alignment and coherence across our bids. We have also commissioned Gartner to independently assure our costs within the IT and Telecoms, Digitalisation, and Cyber Security parts of the GD3 Business plan and they have confirmed that all our costs are realistic and within the ranges they would expect when benchmarked against their large database of reference case studies globally. We have separately submitted Gartner’s assurance report in support of these business plans.

Appendix: Glossary of Terms

Term	Definition	Description
API	Application Programming Interface	A set of rules for how software components interact, allowing systems to communicate.
Asset Management		Tracking and managing company assets, such as hardware, software, and other IT resources.
AWS	Amazon Web Services	A cloud service provider offering various online infrastructure services.
CI/CD	Continuous Integration/Continuous Deployment	A method for frequently updating applications through automated processes.
Cloud		Online storage and services accessible over the internet instead of local computers or servers.
Cloud Environments		Different types of cloud setup, such as public, private, hybrid or multi-cloud, which have different attributes, benefits and challenges that need to be considered when developing a cloud strategy.
Cloud Migration		Moving applications, data, and services from on-premises to cloud-based infrastructure.
COTS	Commercial Off-The-Shelf	Ready-made software or hardware available for purchase and use without custom development.
Cyber Threat		Potential malicious activity aiming to harm or steal data within an IT system.
Data Flows		The movement of data between systems, databases, and users.
Delta		Difference or change, often used in updates or modifications to systems or data.
Disruptors		Innovations or technologies that significantly change or disrupt existing processes or markets.
End User Compute		Technology solutions focused on end-user access and use of computing resources.
End User Devices		Devices like computers, phones, or tablets that users interact with directly.
ERP	Enterprise Resource Planning	Software or services that support the management of finances, human resources and purchasing in an enterprise.
Firewall		A security system that monitors and controls incoming and outgoing network traffic.
IaaS	Infrastructure as a Service	Cloud-based infrastructure provided by a third party, like virtual servers and storage (e.g., AWS).
Infrastructure		The core framework that supports network operations, including hardware, software, and connectivity.
Integration		Combining various systems or applications so they work together seamlessly.
IoT	Internet of Things	Network of physical devices connected to the internet.
Lift and Shift		Moving applications to the cloud with minimal changes to their original setup.
Operational Platforms		Systems or software that run essential business operations, like databases or ERP systems.
PaaS	Platform as a Service	A cloud-based platform for developing, running, and managing applications.
Patching		Updating software to fix security vulnerabilities or improve functionality.
SaaS	Software as a Service	Software accessed online, hosted by a third party, like Gmail or Salesforce.
SASE	Secure Access Service Edge	A networking and security technology that provides a cloud-based platform to connect users, systems, and endpoints to resources and applications.
Vendor		A company that provides goods or services to another business.
VPN	Virtual Private Network	A secure, encrypted connection that allows remote access to a private network.
VOIP	Voice Over Internet Protocol	Technology that allows voice calls using the internet instead of traditional phone lines.
Workflow		The sequence of tasks or processes needed to complete a business function.
ZTNA	Zero Trust Network Access	A security model that requires strict identity verification for each person and device.