Annex

A20.06 Infrastructure Hosting Services Engineering Justification paper

December 2019

nationalgrid

As a part of the NGGT Draft Business Plan Submission

Engineering Justification Paper Hosting			
Asset Family	IT Infrastructure – Hosting		
Primary Investment Driver	System Health		
Reference	NGGT_A20.06_Hosting		
Output Asset Types	IT Storage and Compute services Data Centres Cloud Services		
Cost	£71m		
Delivery Year(s)	2021-2026 (ongoing annual investment infrastructure and cloud services)		
Reporting Table	GTO 3.07, GSO 3.08		
Outputs included in RIIO T1 Business Plan	Nil		
Spend Apportionment	**T1**	**T2**	**T3**
	-	£71m	-

Contents

1 Executive Summary

In Information Technology (IT) terms, hosting is the generic terminology used to cover several technologies such as Storage and Compute. These technologies may be hosted in a physical Data Centre owned and operated by National Grid or by a 3rd party and may be hosted remotely in either Public or Private Cloud. These environments are accessed by a network connection from National Grid.

At the beginning of the RIIO – T1 period National Grid responded to the challenge from Ofgem in setting our allowances to deliver efficiencies by extending the asset life of much of the hosting technology in its estate, reducing capital investment in replacements and thereby generating savings for the consumer. As the RIIO -T1 period progressed it has become readily apparent through employee feedback and performance data that the aged technologies in the National Grid estate have become a serious blocker to performance and productivity. Over the same period, the escalating threat of cyber-attack on our IT systems meant that we had to look again at how we managed our infrastructure so that we could proactively monitor and remediate cyber threats and ensure IT systems and solutions continued to underpin the productivity of our workforce.

In 2018 National Grid re-examined the asset health policies governing all areas of IT technology refresh, leading to a revision of those asset health policies. These policies have been externally benchmarked by Gartner, a leading authority on IT and IT benchmarks. The revised asset health policies led to increased investment in IT infrastructure, resulting in investment above our RIIO-T1 allowances.

The investments proposed in the RIIO T2 period will continue to maintain the asset health of the IT estate in line with the asset health policies and enable us to deliver the work our stakeholders and customers have told us they want us to do.

One of the key learnings we must take from the RIIO T1 period is that the perceived savings from extending core IT asset life can prove to be false economy in the longer term. The impact on productivity, efficiency and customer satisfaction is felt across the whole organisation when IT infrastructure impedes the adoption of new operational technology or software updates. Investment in new applications and tooling can only deliver the benefits designed if the underlying infrastructure is able to provide effective environments.

To support the business ambition and deliver on the expectations of our customers and stakeholders we need to complete the programme of infrastructure modernisation started during the RIIO T1 period and continue to invest to maintain modern, cyber secure and performant infrastructure. We have identified and evaluated a range of options to meet our hosting requirements and concluded that a hybrid cloud approach is the most effective and economically efficient approach. This builds on the provision of several services on the Azure cloud network which started in T1. We propose investment of £71m across the RIIO T2 period to modernise and maintain our hosting infrastructure, enabling us to continue to deliver a safe and reliable network and services to our customers and stakeholders.

2 Introduction

Hosting is the terminology used to describe the Compute and Storage environments on which the applications used within the business run. We can think of these components in a similar way to the components of your desktop or laptop computer. There is some form of Operating system (Windows 10), storage (the hard drive you store your data on), and Compute (the processor and memory that respond to the instructions you give). For your desktop or laptop computer these component parts are contained in a single case, which also provides the power supply and cooling. For an enterprise, these components are scaled up to the level required in the form of a Data Centre.

Effective and efficient hosting environments are vital to a large-scale enterprise such as National Grid, providing the underpinning infrastructure on which data is stored manipulated and processed. The operational processes and business decisions are grounded in facts derived from the proper organisation, manipulation and presentation of data. Inefficient, poorly performing or unreliable hosting infrastructure represents a significant drag on overall organisational performance.

To create clarity in this document, the following terminology will be used to define Cloud types. While these are industry terms; the specific definitions may change subtly from provider to provider.

Public: The public cloud is defined as computing services offered by third-party providers over the public Internet. Customers typically pay only per usage for the CPU cycles, storage, or bandwidth they consume; although pre-buying is an alternative option. Familiar public clouds include Microsoft Azure, AWS, and Google.

Unlike private clouds, public cloud providers purchase, manage and maintain the infrastructure used. They are held responsible for all management and maintenance of the system. They have significant scale as they target tens of thousands of customers. The public cloud can be as secure as managed private cloud implementation if the provider uses proper security methods.

Private: The private cloud is defined as computing services offered primarily over a private internal network and only for a single company. Private cloud computing gives businesses many of the benefits of a public cloud - self-service, some scalability and some elasticity - with the additional control and customization available from dedicated computing infrastructure hosted on-premises. Security posture may be better as company firewalls and internal hosting to ensure operations and sensitive data are not accessible to third-party providers. Internal IT departments are held responsible for the cost and accountability of managing this estate and thus require the same staffing, management, and maintenance expenses as traditional data centre ownership.

Within both cloud types, there are different ways to accommodate the technology requirements. Infrastructure as a Service (IaaS) defines infrastructure resources such as compute, network, and storage as a service. Platform as a service (PaaS) defines simple cloud-based applications as well as sophisticated-enabled enterprise applications.

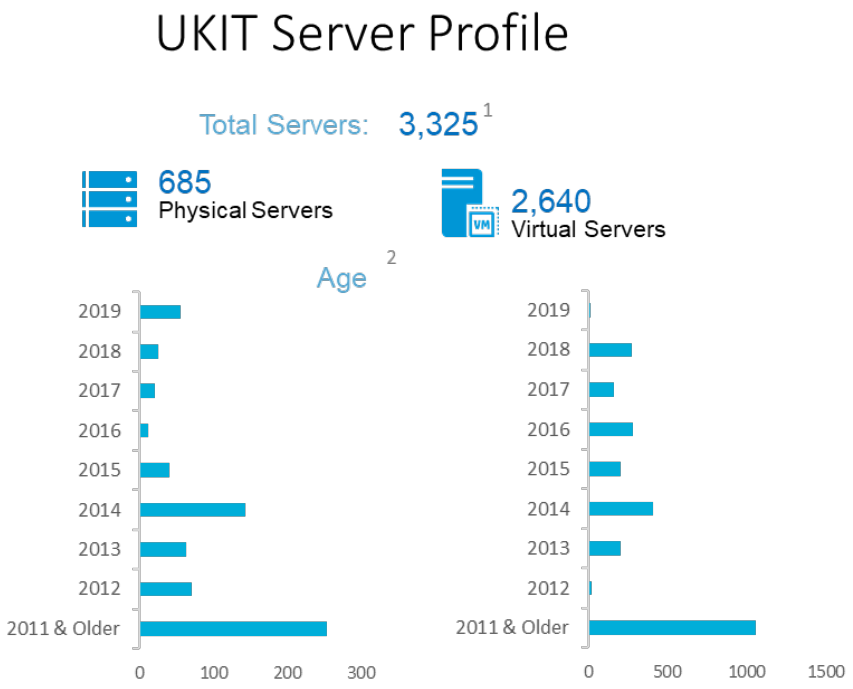
Private clouds can be combined with public clouds to create a hybrid cloud, allowing the business to take advantage of cloud bursting (using public cloud to meet spikes in demand that are too great for the private cloud that is normally used for the service) to free up more space and scale computing services to the public cloud when computing demand increases.

National Grid's business plan proposals for the RIIO -T1 period included requested allowances for maintaining the asset health of IT infrastructure. In setting allowances below the requested level, the Regulator set the challenge to deliver IT infrastructure services more efficiently. We responded to this challenge by seeking to procure services more efficiently and reassessing our IT asset health policies; extending the technical lives of our IT infrastructure assets and accepting higher levels of risk whilst seeking to maintain levels of performance and availability.

As we continued through T1, our employees fed back that our IT was becoming a significant blocker to their effectiveness at work. The increased levels of frustration with IT was evidenced through a dip in our December 2018 cNPS score. This was also one of the causes for the Enablement score from our 2019 Employee Opinion Survey dropping to 57 compared to a score of 73 for a high performing norm. IT equipment and IT systems were two of the top three areas commented upon.

Over the same period, the escalating threat of cyber-attack on our IT systems meant that we had to look again at how we managed our infrastructure so that we could proactively monitor and remediate cyber threats and ensure IT systems and solutions continued to underpin the productivity of our workforce.[1]

With a significant proportion of the National Grid enterprise IT hosting assets at or beyond end of life, the growing cyber threat and the increasing risk of end of life failure has forced us to re-examine the asset health policies applied to the underpinning infrastructure supporting the operational businesses. The revised asset health policies have led to increased spending on IT hosting technologies, mitigating risk, driving improved operational performance and reducing operating cost.



1. Includes Production & non-Production Servers

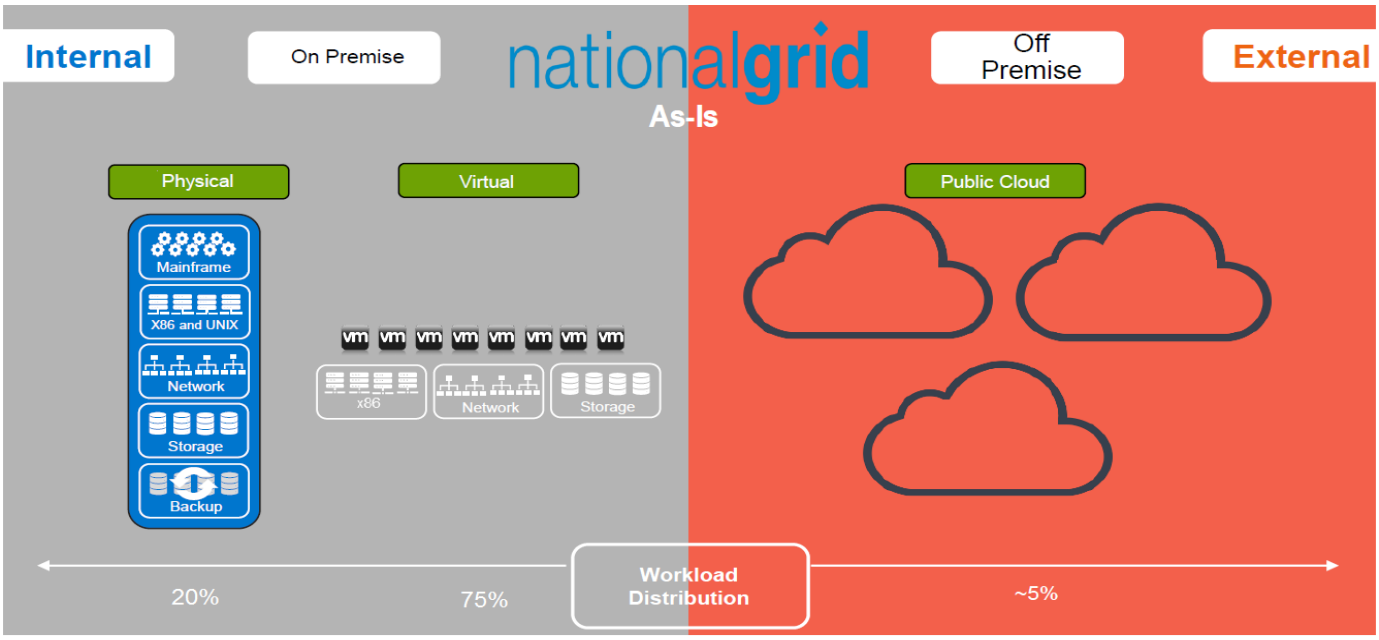
2. Based on first deployment date.

Given the standard expected life for IT server assets is 2-7 years (based on Gartner information), the vast majority of our assets are at or close to end of life (EOL). This is a key driver to the programme that is considered in this Justification Report.

The current [As-Is] estate as quantified above consists of internally hosted and managed physical assets, virtual assets hosted either internally or by third party, and Public Cloud. The diagram below illustrates the “as-is”

[1] The cyber threat faced by National Grid is discussed in more detail in the separate cyber policy and investment justification reports.

balance between physical and virtual on-premise hosting and cloud-based solutions, and highlights the relatively low levels of cloud adoption within the existing infrastructure, at just 5%.



As the UK strives to reduce and eliminate the carbon impact of the energy sector, the energy utilities are working through a period of significant change. National Grid is undergoing a technological and digital transformation, driven by our vision of meeting the needs of customers, stakeholders, and communities in a rapidly changing, and increasingly competitive, energy landscape. IT plays a vital role, by enabling us to optimise operational performance, identify and realise opportunities to grow, and be better equipped to meet customer and stakeholder expectation in the future.

The IT solutions that underpin our operational business units are a vital part of the eco-system that delivers those safe, secure and reliable energy networks, enable the innovations our customers are asking for, enable our ability to react to regulatory change and facilitate efficient and effective operations. Without the investments required to modernise and maintain up-to-date fit-for-purpose IT solutions, the initiatives required to meet our customer and stakeholder requirements will be severely compromised.

The full range of solutions for operational platforms, from energy balancing and SCADA platforms to analytical modelling such as digital twins are all dependent on modern high-performance operating environments. Failure to invest in the hosting environments that underpin our operations will prevent successful implementation of these new operational solutions, reducing the data available in managing the energy networks and markets, with the potential to impact end consumers through deterioration in service and increased energy costs.

As outlined in the main Business Plan, our stakeholders and customers have told us they want safe, secure and reliable networks, efficient energy market operations and greater transparency of data and protection from external threats. Delivering on our customer and stakeholder expectations is dependent on IT solutions that can achieve the customers' requirements whilst keeping data secure and maintaining regulatory compliance.

To support our Security teams in protecting National Grid, and the networks and markets it operates in, it is vital that the core IT assets are fully supported, patched to protect from known vulnerabilities and monitorable by the cyber security technologies we deploy. Failure to complete on the work started in the RIIO T1 period to modernise and maintain the hosting infrastructure would compromise security and performance and limit our capability to provide a high-quality service to our customers and stakeholders.

3 Optioneering

We have identified four options for the management of core IT assets as we move towards the RIIO -T2 period:

1. Continue with the approach inherited from RIIO-T1, making minimal investments to replace defective devices and only providing new assets to meet additional demand. (Minimal Investment)
2. Move existing applications and services to public cloud providers as fast as possible and adopt a cloud only strategy for new services.
3. Exclusively adopt private cloud, ignoring public providers such as AWS or MS Azure.
4. Develop our existing strategy by investing in and optimizing on premise infrastructure and develop our hybrid and cloud capabilities for connectivity and integration.

Evaluation Criteria

We identified the following criteria as important for the assessment of the four options identified in the Justification Report:

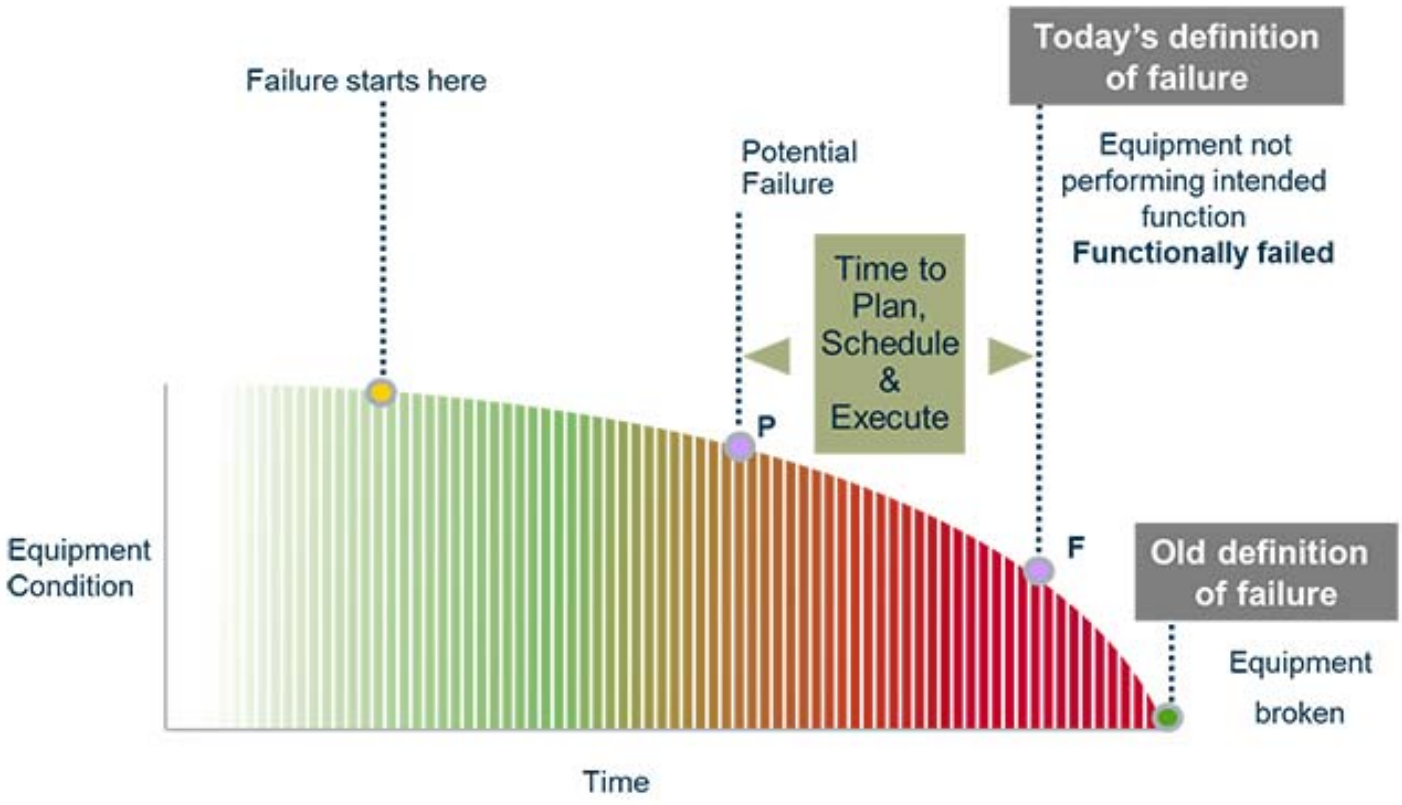
- Total cost of ownership – capital investment and associated operating costs borne by consumers and the need to ensure value for money
- Capacity to deliver - the level of risk associated with the ability of NG and its supply chain to deliver the option
- Business/strategic fit - the alignment of this option to our overall business direction
- Addressing the problem – how well the option resolves the identified issue
- Risk – the overall risk to the business associated with this option

The following sections highlight some of the key issues linked to assessment of each of the options while the table at the end of the section summarises each of the options against the five criteria.

1, To continue with the approach inherited from RIIO -T1 would minimise investment in the short term by continuing to 'sweat' existing assets. This would however also represent the maximum risk option as unlike many capital assets within the energy networks with designed asset life in the order of 40+ years, IT assets have a typical design life of 2-7 years. A significant proportion of the core IT estate is beyond end of life, this increases the risk of absolute failure, but more importantly it indicates that these devices are unlikely to be meeting all functionality and security requirements effectively.

Where part of an integrated IT estate of aged devices is no longer supported with updates, or identified vulnerabilities are left unpatched, we create the potential to constrain the entire estate due to compatibility issues between updated and legacy software revisions. Failure to use the full functionality delivered with modernised fully patched and updated IT hardware will compromise the security, effectiveness and efficiency of the entire IT ecosystem and the business processes it supports.

The diagram below seeks to demonstrate the changing definition of failure in IT infrastructure. It is no longer simply the point at which a device fails to operate, but much more commonly regarded as the point at which a device no longer meets the evolving functionality requirement. Where failure is recognised as the gradual erosion of functionality, replacement is required at the point at which functionality is materially compromised, not the much later point where all functionality has deteriorated to the point of absolute failure. This may be a result of increasing performance requirements or enhanced functionality requirement. The diagram also recognises that the time to implement replacement of infrastructure is before the functionality or performance characteristics impact the effective operation of the business.



2, The opportunity to outsource IT Infrastructure to Public Cloud may seem like a good idea, and the potential benefits may appear compelling. The real cost of handing over control of IT infrastructure to external providers may prove to be more than the potential benefits can support.

To plan moving all application hosting to Public cloud provision quickly would fail to recognise some potential issues with data security, sovereignty and performance. From the security perspective some of the data managed by National Grid is sensitive in nature and would require extra consideration before a public cloud solution could be approved as acceptable. Beyond the initial security consideration, some sensitive data may also have data sovereignty compliance requirements that need careful management within the concept of a public cloud. Restrictions on data hosting in other jurisdictions becomes much more difficult to verify, making regulatory compliance a complex task.

The complex real time applications National Grid utilises in the management of energy markets and networks place high demands on operational performance, with specific configuration requirements not catered for in the "one size fits all" multi-tenancy public cloud environments. Within these public cloud environments control is ceded to the hosting provider, often requiring all users to maintain their estate fully patched and at latest revisions of operating systems. The levels of testing required to approve software updates to operating systems before migration of critical systems may prove impossible within the cloud providers time frames, but with the adoption of public cloud the IT function loses direct control or influence of this timetable, potentially causing critical infrastructure applications to be migrated to untested environments.

Financial forecasting and control of operating costs becomes increasingly complex, with many cloud models adopting a "pay as you go" operating model, where a detailed understanding of the likely volumes of data moving to and from the cloud becomes critical.

3. The option to adopt an exclusive private cloud

Adoption of private cloud brings many advantages over traditional physical hosting in terms of automation and orchestration.

To completely ignore the potential benefits of Public cloud would represent a dereliction of our duty to the consumer. There are without doubt scenarios where hosting in the public cloud represents the best solution in terms of both cost and operational performance and efficiency. Examples of this are in the growing range of solutions provided on a Software as a Service (SaaS) basis, where the software vendor supplies the solution on a subscription-based model, also hosting the application on its infrastructure. Solutions provided in this way are hosted on platforms optimised to the specific application requirements, updated routinely by the product vendor to ensure that the benefits of the latest updates are realised as soon as possible.

Table 1: Assessment of options considered

Option	Total Cost of Ownership	Capacity to Deliver	Business / Strategic Fit	Addressing the problem	Risk	Overall
Do nothing	**Red** High contract and support costs are expected if contract renewal were optioned.	**Green** Use existing skills and resources. Current Contract expires with DXC in 2021	**Red** Unable to leverage leading industry solutions and ability to change and innovate severely impacted	**Red** Does not address customer experience and resilience	**Red** Costs to host and manage would increase significantly and high risk to service due to end of life hardware and software.	Rejected
Fully outsource (SaaS & Public Cloud)	**Red** Highest cost	**Green** As commodity services, external companies bring economies of scale, best in class services and innovation.	**Green** Minimal effort to run and maintain systems and ability to leverage leading edge services for rapid change and innovation	**Amber** Addresses customer experience, capacity and resilience requirements	**Red** Costs to acquire services would increase and will be difficult to manage. Challenges with CNI workloads and alignment	Rejected
Fully insource (Private Cloud)	**Amber** Higher costs due to costs of insourcing, training and operations	**Red** Difficult to acquire skills required to build out the environment. Time and resource requirements also considerable for a full private cloud build out	**Red** Limits ability to leverage leading industry solutions and ability to change and innovate severely impacted	**Green** Addresses the resilience problems but will have limitations in meeting customer needs	**Red** Ability to acquire skills and build out environment a major concern and being able to provide the required level of resilience and capacity	Rejected
Mature Hybrid (preferred option)	**Green** Best cost profile based on mix of investment costs and optimized capabilities to support	**Green** Repurpose existing resource for new on premise environments. Cloud services where appropriate leveraging cloud vendors	**Green** Enables the optimum balance of differentiating on premise and commodity services	**Green** Addresses customer experience and resilience requirements	**Red** Sub optimal blend of cloud services and on premise increases costs	Recommended

4. National Grid has assessed the future requirements, considering the feedback we have received from our customers and stakeholders, the requirements of the business and the need to modernise the existing estate, we have concluded that no single solution will meet all requirements.

The most effective solution to meet the totality of our hosting requirement is a hybrid of a number of technical solutions, including subscription-based services (SAAS), public and private cloud solutions. This is in line with the recommendations of the Gartner report which included using public cloud to meet peak consumption and to allow greater flexibility.

Subscription based, SAAS solutions are becoming ubiquitous in many sectors including ERP and CRM systems. This approach to many common business applications brings with it many advantages, with the hosting environment optimised to the application, delivering good application performance. Routine software updates to both the hosting environment and the application stack are tested and applied as part of the subscription.

Public cloud, while not appropriate or desirable for all applications, will retain a significant role in meeting our future requirements. Specific criteria will be utilized to determine suitability of public cloud to meet security, cost and performance objectives.

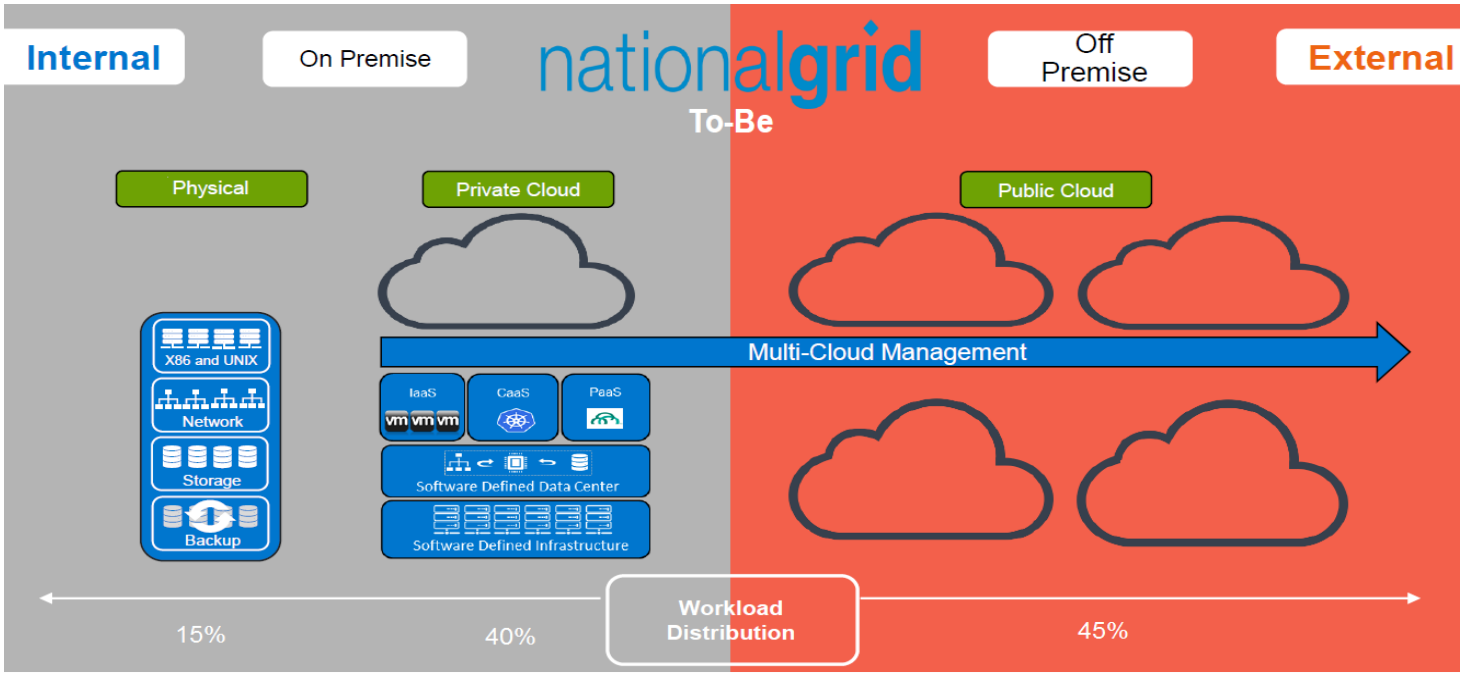
The investment made in Data Centre technologies as part of the strategic CNI data centre programme has created potential capacity for the development of Private Cloud hosting. New technical solutions such as hyper-convergence is shrinking the equipment power and cooling requirements, making on-premise private cloud solutions more viable. Hyper-convergence enables linear scaling of compute and storage capacity and reduces reliance on separate network and storage resources because the traditional hardware infrastructure elements are software defined.

We have initiated a competitive process to assess and select the most suitable hosting provider based on our requirements and vision for our hybrid cloud future. We will award a contract in the current regulatory period that will be due for renewal within T2. During this time, we will be constantly assessing the market to ensure that our chosen hybrid strategy is optimal, is taking full advantage of developments in the market and will adjust our strategy and placement criteria as appropriate. Closely aligning on and off-premise deployment architecture will also give us the flexibility needed to adapt and to tender for other services if needed. [This process has allowed us to generate the estimate of the cost for hosting which will be ultimately determined through the process we have initiated.]

Target end state for preferred option

To deliver the target [To-Be] end state we will use agents to understand the current estate and interactions between systems to inform logical move blocks. There will be a progressive migration of services to their optimum hosting model, starting in T1 these migrations will be aligned to major change programmes to avoid unnecessary disruption and cost. Diagram 4.1 below shows how workloads are planned to be apportioned across the various hosting models through the T2 regulatory period

Diagram 4.1



The resulting hosting environment will need all complementary aspects of networking and security to be provisioned and will be optimised for the current application estate. We will continually optimise our infrastructure requirements through the following:

1) Application rationalisation, optimisation and decommissioning, coupled with data archival and removal (in line with legal and company policies)
2) Use of SaaS where available as a Public Cloud option, where our processes are sufficiently standardised and there are commodity services, SaaS will provide cost-efficient optimised delivery of IT services to business users
3) Modernise our applications with appropriate solution designs which recognise newer infrastructure technologies and associated cost of storage and compute infrastructure
4) Dynamic provisioning and ongoing consumption management to ensure only the resources required are used at any moment in time. This will include further flexibility to meet normal and peak workload demands.

4 Detailed Analysis & CBA

A typical cloud strategy looks at people, process, information and technology across applications, client services and infrastructure services. Implementation usually occurs in three phases, modernization, optimization and transformation.

In reviewing the future hosting requirements four main options were considered:

- Make no investment, continue to extend the asset life of existing infrastructure.
- Move all application hosting to Cloud based solutions
- Develop fully inhouse private cloud
- Adopt hybrid of public and private cloud

Table 1 above outlines the qualitative assessment of these options.

In summary, we have examined the option to make minimal investments and continue to extend the asset life of the existing asset base. There are several issues with this, not least the commercial and contractual position with the existing provider. This contract is in the final year having consumed the options to extend, we therefore must return to the market with a competitive procurement event in order to remain compliant with EU procurement regulations.

Full public cloud adoption fails to meet the technical needs in some circumstances particularly where data sovereignty, or compliance criteria require assurance of specific geographical hosting location. There are many circumstances particularly where there is high volatility of data where the operational costs of public cloud can become unstainable.

To completely ignore public cloud (in the right circumstances) would be turn our back on the considerable benefits associated with agility and saleability. Build out of exclusively private cloud requires significant capital expenditure, requires specialist skill sets that are difficult and expensive to secure and demands large volume of high quality data centre space with all the associated power and cooling plant requirement.

The Hybrid solution (our preferred solution) allows us to leverage the benefits of each solution by careful selection of the appropriate hosting strategy for each application on a case by case basis. Protecting highly sensitive data in our own private cloud, hosted in National Grid facilities while leveraging the public cloud for more commodity applications we optimise the hosting solution and with that deliver the most cost effective strategy.

To ensure that the level of investment required for our recommended option is correct we have extensively market tested it in line with industry best practice and norms referring to Gartner, a recognised expert in IT benchmarking. Gartner indicate that our asset health policies are in line with industry practice, and the value of investment is within the benchmark range.

The investment costs profile and associated benefits is set out in the table below.

£m	2022	2023	2024	2025	2026	Total
Preferred Option - Costs	-30.65	-11.66	-9.40	-14.50	-4.50	**-70.71**
Preferred Option - Benefits	12.00	8.00	2.00	2.00	2.00	**26.00**
Net Cost	**-18.65**	**-3.66**	**-7.40**	**-12.50**	**-2.50**	**-44.71**

Key Benefits of our chosen strategy include:

- Ability to leverage market investment in commoditised cloud services
- Improved resilience from public cloud through enhanced deployment models available from cloud platform providers, for private cloud from standardised hardware and common availability processes and technologies
- Enhanced agility and flexibility for workload deployment supporting digital initiatives
- Cost avoidance through automation enabling National Grid to scale and absorb new workloads and contain costs in provisioning and decommissioning
- Improved protection of the energy network through deployment consistency and leveraging vendor best practice and certification to improve cyber and technology risk
- Financial and non-financial benefits, through improvements in enforcement of standards, policies, and cost transparency from charge-back for better informed technology decisions

To fully realise the benefits, we will need to move from expensive platforms to commodity hardware, for example moving from AIX onto Linux. This could take 3-5 years for most applications to be migrated, as this would be tied to other application roadmap events (apps refresh or replacement). Given the current level of technology and market maturity, we currently view public cloud as not appropriate for strictly confidential and CNI data. This position may change as cloud technology and security improve. Where possible we will leverage cloud hosting to harness scale and availability for IT services.

Detailed CBA is attached as annex A to this justification report: NGET_A14.03a_Hosting. CBA results are summarised in the table below.

Option	NPV @ 2.9%
Baseline	-82.8
Preferred Solution - Hybrid Cloud	-42.2
Private Cloud	-92.6
Public Cloud	-74.6

The attached Cost Benefit Analysis (CBA) sets out quantitively in cost terms the comparison between the options available and demonstrate that while public cloud represents the lowest cost in terms of capital investment, the operation “run the business” costs are high. Conversely, as might be expected, a wholly private cloud solution represents a significant capital investment. The hybrid solution facilitates the flexibility to balance between Capital investment and operational cost, delivering the optimum outcome in terms of Cost.

The table below includes sensitivities for a 5% discount rate, and costs at plus and minus 10%. This indicates that the preferred solution is resilient to a credible level of change.

£m	NPV @ 2.9%	NPV @ 5.0%	Costs - 10%	Costs +10%
Preferred Solution - Hybrid	-42.21	-43.46	-35.49	-48.92

The combined balance of quantitative and qualitive assessment concludes that development of a hybrid of hosting technology options, create the ability to actively select the optimum solution on a case by case basis as part of the business case development and architectural design as new applications are proposed. This assessment methodology will also be applied as we look to update hosting of the existing application estate as the current contract comes to an end ensuring that National Grid full optimises the hosting infrastructure delivering the best blend of capability and cost in each case.

5 Key Assumptions, Risks and Contingency

A key assumption is that a critical component of a Cloud Strategy is taking a software-defined approach, the following details several of these assumptions:

- Compute resources should always be deployed as virtual machines, leveraging a common hyper-visor.
- Compute & Storage resources should be hosted on Hyper Converged Infrastructure (HCI) and all storage should be software defined.
- Where possible, Network resources should also be deployed as software defined in a zero-trust model. This will allow greater flexibility, control and security when connecting public and private clouds.
- There should be a control plane to manage the full lifecycle of workloads, as well as an API layer to shift the consumption of hardware as software.
- Resources should be deployed and consumed as *services*.

We have also identified several risks in the table below that require solid mitigation plans to ensure the successful delivery of our commitments in the T2 regulatory period

Risk	Mitigation
Suppliers will not be able to deliver the services at the price agreed	Extensive procurement process and analytic analysis gives confidence that suppliers have a proven track record and can deliver value to National Grid
Strategy will not be defined and executed optimally due to National Grid not having the retained capability or key skills to define new patterns for use introducing additional risk of having to re-design at additional cost	Global IT has strengthened the capability of its architecture and operational teams. The selection and transition of services is being undertaken by employees who will select, implement and maintain these services going forward. We will also supplement resource with our framework of contractors and partners. Key decisions will be reviewed by our central Architecture Review Board and Infrastructure & Operations delivery teams.
Age of current estate may make migrations challenging or unachievable. May force application modernisation or other technology solutions	Agent based assessments couple with application estate assessment of existing environments is being undertaken to better anticipate any risks and limitations.
New services not available in timely manner to facilitate exit from existing contracts	Work has already begun to prepare for new hosting models and any required contract exit. We are regularly reviewing utilization and capacity
Lack of automation in provisioning; continued use of old Ways of Working; not designed for rapid scaling resulting in not being able to react to future project requirements.	Organization is implementing a new operating model to focus on automation, update processes and ways of working and bring in key skills to meet future demand.
Ability to host legacy applications / technologies	Provision will be made in new contracts to allow for a percentage of legacy systems

Age of current estate may make migrations challenging or unachievable. May force application modernisation or other technology solutions	Agent based assessments couple with application estate assessment of existing environments is being undertaken to better anticipate any risks and limitations.
New services not available in timely manner to facilitate exit from existing contracts	Work has already begun to prepare for new hosting models and any required contract exit. We are regularly reviewing utilization and capacity
Lack of automation in provisioning; continued use of old Ways of Working; not designed for rapid scaling resulting in not being able to react to future project requirements.	Organization is implementing a new operating model to focus on automation, update processes and ways of working and bring in key skills to meet future demand.
Ability to host legacy applications / technologies	Provision will be made in new contracts to allow for a percentage of legacy systems

6 Dependencies

To implement the proposed hosting solution and deliver the efficiencies associated, it will be vital to also implement the enterprise networks modernisation proposed. Without modernised network capabilities it will not be possible to migrate applications and platforms to public cloud or subscription-based services (SaaS) in the volumes proposed. Leveraging the ability to reduce operational costs by adopting public cloud where desirable is fundamental to achieving the 1.1% year on year efficiency commitment.

7 Conclusions

To identify the requirements for hosting we have assessed and understood our current and longer-term hosting requirements, examined the market and tested our approach commercially and technically. We have listened extensively to our users and stakeholders, developing a strategy to provide effective, fit for purpose and efficient hosting services.

Our strategy is to continue to mature our hybrid cloud model. We started this journey prior to RIIO T2 by building several key services on the Azure cloud platform and commenced a hosting request for proposal to re-contract our main hosting services. We have revised our strategy, reviewed and reinforced our policies and governance bodies to assess workloads for optimum deployment, and created a cloud framework to guide execution. We have started and will continue to build the architecture to enable our hybrid strategy, including connectivity and integration and will architect services to build-in flexibility for future change. Implementation of modern, secure and efficient hosting services, enabling us to operate a safe and reliable network and meet the expectations of our customers and stakeholders will require investment of £71m during the RIIO T2 period.

The combination of modernised hosting and network services full underpin the wider IT strategy to deliver up to date effective and efficient services enabling the wider National Grid business entities to achieve reach and operate at the efficiency threshold.

8 Outputs included in RIIO T1 Plans

Nil