Investment Decision Pack

NGET_A14.20 – IT Operations and Tooling

December 2019

As a part of the NGET Business Plan Submission

nationalgrid

Engineering Justification Paper IT Operations and Tooling			
Asset Family	IT Infrastructure – Operations		
Primary Investment Driver	Sustainable IT Operations		
Reference	NGET_A14.20_IT Operations & Tooling Digital IT Operations		
Output Asset Types	IT Infrastructure Applications		
Cost	£52m		
Delivery Year(s)	2021-2026		
Reporting Table	ETO D4.3A		
Outputs included in RIIO T1 Business Plan	Nil		
Spend Apportionment	**T1**	**T2**	**T3**
	-	£52m	-

Contents

1 Executive Summary

National Grid owns and maintains the high-voltage electricity and natural gas transmission networks in England and Wales. We move electricity and gas from where it's generated, through their respective systems, to our direct customers and to the distribution companies who deliver that power to homes and businesses. Our IT Operations are a key component of our ability to deliver energy reliably and efficiently.

Currently, our IT Operations have limited visibility into real user experience, we lack real-time data on end-to-end application performance, topological dependencies and financial information. Consequently, application maintenance is labour intensive and could be more efficient. Resources are dissipated on manual operational effort with limited return. We don't currently design for "automation first", so an incremental approach will miss the opportunities afforded by end-to-end monitoring and intelligent-operations management tools.

This paper specifically addresses the above concerns and relates to our investments in IT Operations over the RIIO T2 period. It describes in more detail one of the key pillars defined in our IT Strategy covering our proposed investments for the period as well as our alignment with our stakeholders' priorities and the broader needs of the business. Automation will enable us to balance efficiency and the need for rapid change as we continue to invest in the people, tools and processes needed to execute and manage the Business of IT optimally. As referenced in our IT strategy, *Gartner 2019 IT predicts* cited IT automation as driving many benefits around efficiency, addressing talent shortages and enabling the delivery of data. To ensure we are leveraging these benefits we are focusing on the following areas. Firstly, establishing cloud aware cost transparency for all IT cost across the business enabling accurate decision-making. Secondly, we will invest in tools, automation and streamline our processes so that the IT estate can be managed as cost efficiently as possible across planning, build, provision and maintenance. Lastly, we will invest in the consolidation and automation of the network operations centre to ensure optimized network operations.

This document covers the overall IT Operations and Service Management capability, leveraging requirements from all other RIIO papers, consolidating the strategy to deliver operational performance for all IT services and infrastructure supporting our core business. The guiding principles of our strategy are:

- Bespoke IT solutions are designed to be deployed and operate without manual intervention
- Commodity software platforms (e.g. Office 365) require radically different support models to bespoke solutions

The implementation timeline for the automation of IT operations in T2 is as follows. Short term (0-24 months) introduce full stack performance monitoring, create rich performance data and prove the "No-Ops" concept in a limited portfolio. Medium term (2-5 years) repurpose applications to fit the new model as they are refreshed. Beyond 5 years achieve fully automated IT operations.

2 Introduction

IT Operations encompass the processes and services that are provided by IT to their internal and external customers and used within the IT department to manage the IT estate. This includes the provision of new IT requirements and services, Service Desk and Tech Bar services, operational monitoring of network and server infrastructure, application maintenance and patching etc.

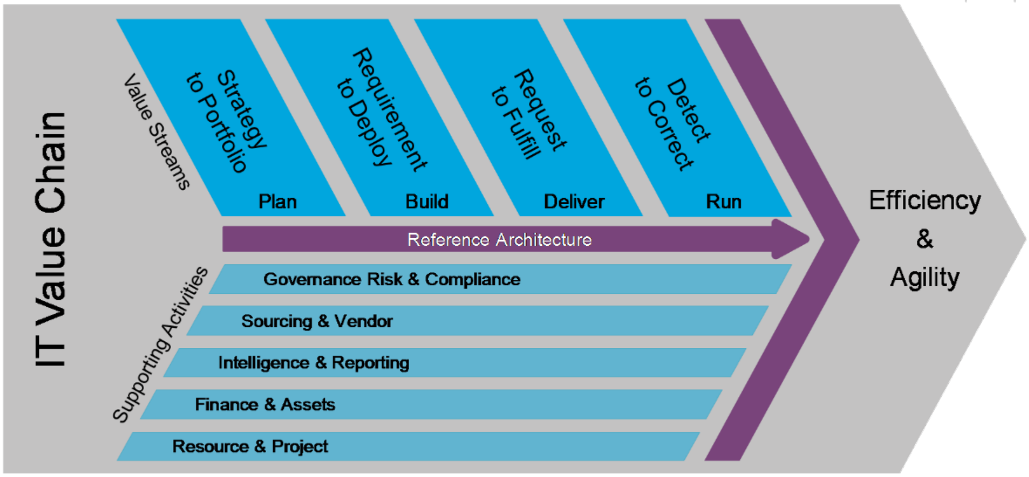
It is increasingly important to provide a frictionless customer / user experience in all aspects of the IT service, ensuring high availability by maximising uptime of the applications users rely on, providing efficient self-serve capability for requesting new services and resolving issues before users are impacted.

To ensure the effective and efficient delivery of services, IT Operations needs a few key technologies and tools.

IT operates sets of inter-related processes to Plan, Build, Provision and Operate the IT services required by our businesses and customers. These are grouped into four principal Value Chains:

- Plan value chain – from understanding business **strategy** to translating it in to a **portfolio** of projects & initiatives that are optimized to add maximum value to our organization and its customers.
- Build value chain – from the **requirements** to **deployment** of new applications and IT services
- Provision (Deliver) value chain – from user/customer **request** through to the **provision** of services to users
- Run/Maintain value chain – the **detection** through to **correction** covering the monitoring, operating and remediation of the services IT provides.

© 2015 The Open Group



[1]

The overall Digital IT strategy is to exploit opportunities to further digitise the operation of each value chain through improved tooling and automation of each process. Our primary approach remains the streamlining of business processes through process re-engineering and using modern platforms – such

[1] The Open Group IT4IT^{TM} Reference Architecture, version 2.1

as ServiceNow and DevOps tools - which support end-to-end processes. However increasing use of automation, robotic process automation (RPA) and machine learning can result in substantial efficiency improvements. The overall objectives are to reduce costs, increase pace and throughput and reduce business risk. Automation is also necessary to manage the increasing scale and complexity of IT. Gartner states "Automation is no longer optional. It is a response to the increasing complexity and scale of next-generation technologies". [2]

Key outcomes from digitising IT include ensuring all participants in the chain have the right access to the right information by improving efficiency. Predictability is increasing and reducing risk through the digitisation of processes, automation of key controls and the removal of manual handoffs. Over time this can result in cost reduction.

During RIIO T1 considerable emphasis was put on improvements to the Provision and Maintain processes working with our strategic partners, which included the establishment of ServiceNow as our primary service, request and incident management platform. This has established the core foundations from which further opportunities arise for digitising IT Operations such as Application Performance Monitoring, automated provisioning, and a centralised Operations Centre.

More recently IT has started to digitise several Build processes such as the use of automated testing and automated provisioning of test, development and training environments. We are investing in DevOps as a step towards Continuous Integration and Continuous Delivery (CI/CD) of new and enhanced services into production.

Alongside this journey, we will integrate security policies and practices into our DevOps culture, and integrate security controls into our DevOps tool-chain. This approach of embedding security at every phase in DevOps to ensure efficient delivery of security requirements is commonly referred to as SecDevOps. The opportunities this approach brings are: reducing costs to deliver secure solutions; closer synergies between DevOps delivery teams and security teams; reduced risk of introducing new vulnerabilities / reduced risk of discovering high scoring vulnerabilities late in delivery. MORE here on SecDevOps journey and opportunities.

Digital transformation offers new opportunities for a business to drive value. The Digital Agenda aims to harness these opportunities for National Grid. To support this approach, IT itself needs a similar step-change to make use of advances in software automation, application performance monitoring and intelligent IT orchestration.

The Digital Agenda is a step change in the application of technology to solve business problems. That same thought leadership can be also be applied to the internal workings of IT to ensure it has the structural coherence to deliver on its promises.

We will apply this digital philosophy to all IT functions, from planning to operations.

[2] Solution Path for Infrastructure Automation, Gartner, July 2019

3 Planning: Digital Planning and Prioritisation

The Plan value chain covers all activities associated with planning the introduction of new or improved IT services. It encompasses understanding the business and IT strategic intents, forecasting future needs, receipt of demands for new or improved services, and their assessment, prioritisation and sequencing against strategic roadmaps per business value, deliverability, dependencies and other constraints. Given the amount of proposed investment over RIIO-T2 period it is critical this is appropriately planned and sequenced to deliver greatest value.

Demand, portfolio, project and architecture management

IT is investing in new tooling to improve planning and prioritisation capability which will 'digitise' more planning functions including strategic planning, demand management, strategic resource planning, financial forecasting, cost management, application portfolio management and technology rationalisation. Consolidating multiple tools into a single platform (and addressing gaps) with a BI 'umbrella' across information sources to make better informed decisions.

The objectives are to make most effective decisions based on real data about the existing and future IT services, their costs, health and configuration. Utilising scenario planning capability to model the impacts of decisions before they are made.

Financial Management & Technology Business Management

As the energy utility sector becomes increasingly digitised, the costs of technology and the decisions taken in IT become increasingly important to the overall efficiency and performance of the industry, directly impacting the consumer. In the past, the mapping of IT spend to direct business outcomes has been difficult and inaccurate.

IT has recently invested in Apptio to give greater insights into the costs of existing services. Our roadmap includes greater integration with strategic planning system and with CMDB as we gain a richer view of IT assets and their health through automated asset discovery, software licence management and cloud access brokers. This will be extended to provide a full 360-degree view of IT Finances which covers both current cost of operation (RTB) and future investment / cost to achieve (CTA) data. Utilising financial management tools also allows more detailed benchmarking of performance against peer groups.

Similarly, there are opportunities to improve lifecycle management and the planning of technology upgrades. Automating the analysis of vendor support lifecycles against our CMDB data, adjusting for risk appetite, allows for improved prioritisation for where and when to invest in upgrades or replacement. Technology business management (TBM) leverages the CMDB data to provide genuine transparency to IT financial performance allowing investments to be focussed to achieve greatest impact.

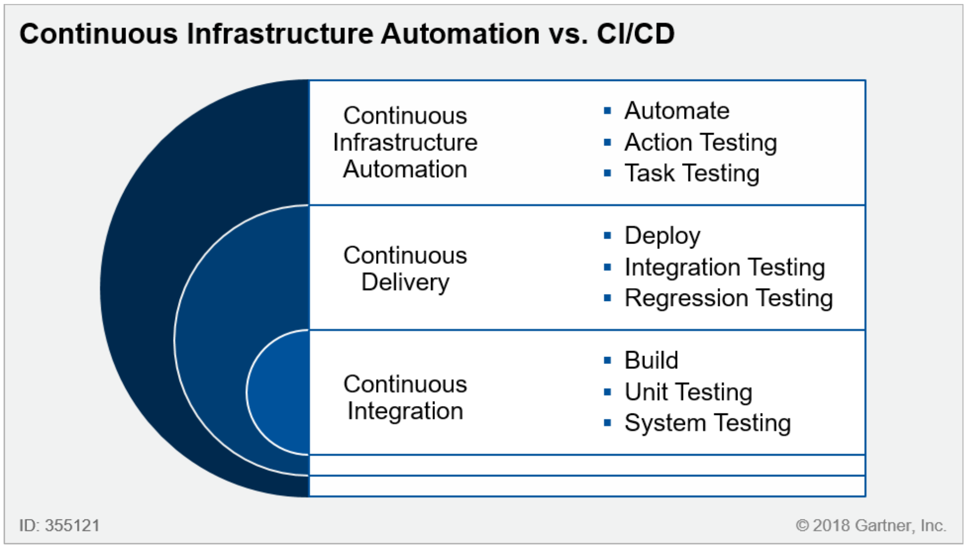
Within a regulated monopoly such as National Grid, Application Portfolio Management and TBM creates the ability to transparently apply consumption based financial modelling ensuring that costs are correctly allocated and driving accountability into the operational businesses for the technology decisions taken by those businesses. These investments will improve traceability and monitoring of progress against the commitments within our strategic plans.

Remove page break?

4 Build: Automating the development and release of services

Development and integration teams are increasingly challenged to respond to demand for more frequent change and are being expected to deliver these quicker. Historically automation has been applied to parts of the development process, such as automated testing tools to execute unit, stress (load) or regression testing. Agile development practices and DevOps processes are increasingly used to further increase the speed of delivery, using DevOps tools which improve speed through integration and automation of development tasks across the DevOps tool-chain.

Within operations the automation of the provision of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) services has similarly been the first step in automation. But other automation opportunities exist and organisations moving to CI/CD which combines build with continuous infrastructure automation. CI covers the building, integrating, testing and delivering of functional changes to applications (software) on a scheduled, repeatable and automated basis. Extending infrastructure automation to support DevOps processes allows for repeatable and scalable CI/CD processes. With CI, software development teams can leverage automated and repeatable build and test processes. Code management, version control, regression testing and deployment are managed. CD extends this from compilation of new/amended software, assembly as a build package, testing and deployment into relevant development, test and production environments within a repeatable framework. This can lead to what Gartner terms as Continuous Infrastructure Automation (CIA), with the ability to deploy any change rapidly, safely and on demand at any time. [3]



Continuous Infrastructure Automation vs. CI/CD

Continuous Infrastructure Automation	▪ Automate ▪ Action Testing ▪ Task Testing
Continuous Delivery	▪ Deploy ▪ Integration Testing ▪ Regression Testing
Continuous Integration	▪ Build ▪ Unit Testing ▪ System Testing

ID: 355121

© 2018 Gartner, Inc.

CI/CD is not appropriate in all circumstances but will increasingly be adopted in areas with high volatility and requirements for rapid change. National Grid aims to adopt CI/CD practices, tools and automation opportunities as they mature.

[3] To Automate Your Automation, Apply Agile Practices and DevOps Tools to Infrastructure and Operations, Gartner, 2018

As our operating model evolves and matures and the IT strategy is executed, we will continue to build and enhance our skill sets for the future. Funding models will support more platform-centric programs which concentrate business unit demand around key platforms (CRM / Salesforce, Asset Management, data platforms etc.). These will require specific investment for build on those platforms but alignment back to IT business management tools will be key to retaining the required transparency. As demand for new technology and approaches comes in through our direct investments, we will also need to continue to develop new skill sets and automation tools for the build phase in areas such as:

- RPA, AI, Machine Learning and data science.
- Design Thinking / User focused design and Lean UX skills and tools for customer journey definition and wireframing
- Continuing to build cyber & DevSecOps skills and tools to embed security in the build phase improving the speed and consistency of cyber protection in applications and services.

5 Provision & Maintain: Digital IT Operations

Provision and Maintain encompasses the processes and technologies used within the IT department (and provided to their internal and external customers) to manage the IT estate. This includes service requests associated with the provision of new IT requirements and services, Help Desk and Tech Bar services, operational monitoring of network and server infrastructure, incident management and application maintenance activities such as patching and upgrades.

It is increasingly important to provide a frictionless customer / user experience in all aspects of the IT service, ensuring high availability which maximises uptime of the applications users rely on. Users expect efficient self-serve capability for requesting new services and for issues to be resolved before they are impacted. To ensure the effective and efficient delivery of services, IT Operations needs a few key technologies and tools.

Digitising IT Operations can be applied to the following areas:

- Application Performance Monitoring / Management
- Application Maintenance
- Provisioning & Orchestration
- Fault Diagnostics and Resolution
- Discovery Tooling
- Security automation

Automation is at the heart of this opportunity. As Gartner puts it … ‘automation is a foundational tenet that allows organizations to cope with the rapid pace and scale of digital business.’ (Gartner - Hype Cycle for I&O Automation, 2019, p. 2). Increasing the role of automation in IT Operations opens the door to accelerate time to value, improve the user experience, and reduce waste by making possible the so called "No-Ops" [4] model where systems need little or no manual intervention to run.

In RIIO-T1 we negotiated new contracts and created an application development and maintenance framework with several key partners. These contracts were written explicitly to drive our partners to automate processes. We will continue to build on this through the T2 regulatory period ensuring alignment between our environments and platforms and those created and operated by our partners.

Digital IT Operations – Application Maintenance Context

The Digital Agenda aims to harness new technology opportunities for National Grid. IT Operations can support the Digital Agenda by using advances in IT Operations technology to reduce waste and enable faster development cycles. Such an operation leverages advances in automation, application performance monitoring (APM) and IT orchestration tooling to create production environments which require less people to run and afford greater insight into performance and increase uptime.

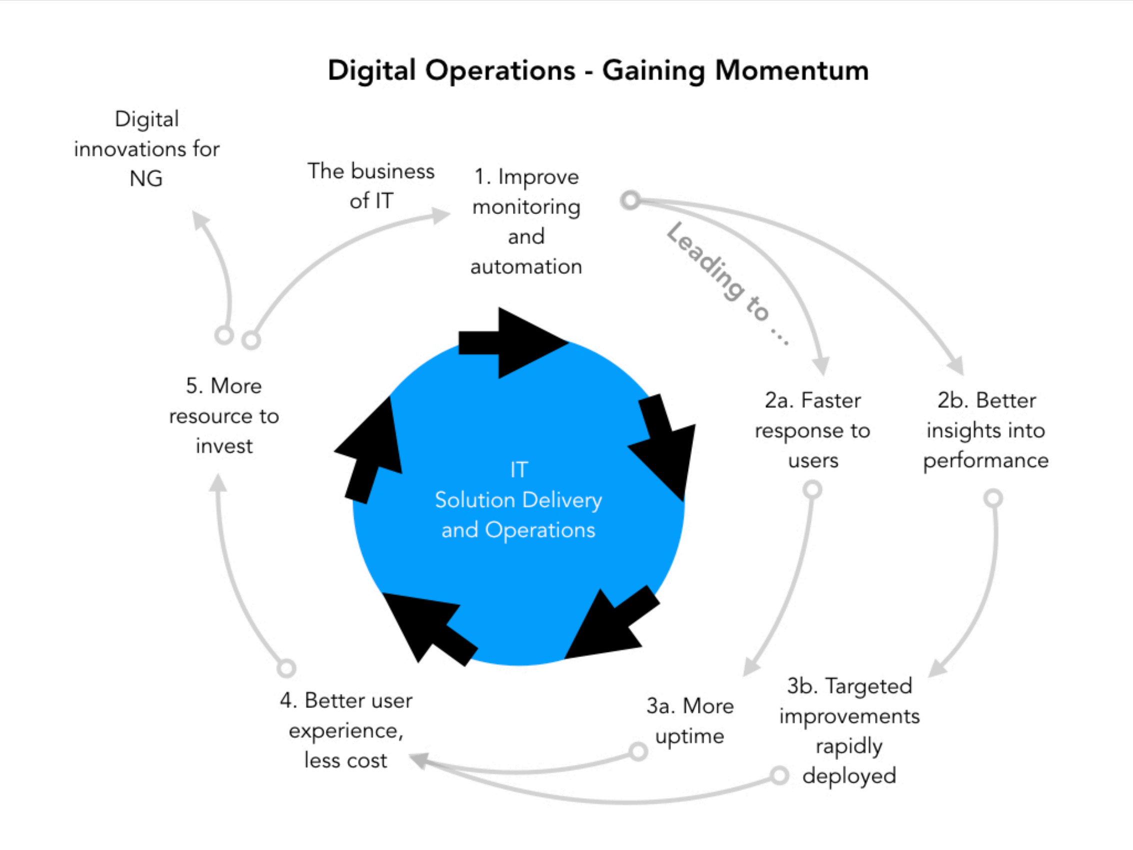
The opportunity is to build environments specifically designed to extract comprehensive performance data and to use this to then drive automation. This enables a long-term goal of a so called "No-Ops" model where systems need little or no manual intervention allowing resources to be focused on value-add activity.

The implications will ripple upstream. Design to Operate principles mandate the non-functional requirements necessary to maximise the benefits of automation and performance monitoring. This ends the ineffective practice of retrofitting tooling. Designing for automation brings benefits throughout the software development lifecycle because it enables rapid progression from build to test to deployment and operations. Such a step-change has the potential for 10X improvement in uptime, accuracy and efficient use of resources [5].

This approach has a cumulative effect creating a virtuous circle that starts with real-time performance data and automation, leading to enhanced user experience and rapid development cycles, which creates more opportunity for innovation and value-add activity.

Our use of automation has already delivered benefits in individual cases. The Privilege User Access Review (PUAR) is one such case with significant man-hours saved by applying Robot Process Automation (RPA). In this case a 2-hour manual task is transformed into a sub-minute RPA driven transaction, enabling what used to be an 80-day audit to be run over night and with greater accuracy.

[4] "According to Gartner's 2018 Hype Cycle for Performance Analysis, DevOps and AIOps are the two areas that have gained the most momentum in the industry. We need to think of DevOps as the beginning of a bigger, business-critical journey towards a more automated future through AIOps and, ultimately, NoOps — the point where an IT environment becomes so automated that a dedicated team isn't even needed for managing tasks anymore." https://www.lumeer.io/devops-to-noops-with-ai-in-2019/


Digital Operations - Gaining Momentum
Digital innovations for NG
The business of IT
1. Improve monitoring and automation
Leading to ...
2a. Faster response to users
2b. Better insights into performance
3a. More uptime
3b. Targeted improvements rapidly deployed
4. Better user experience, less cost
5. More resource to invest
IT Solution Delivery and Operations

This approach is tailored for industry-standard systems and the bespoke solutions which are unique to the energy industry or developed in-house by National Grid and its partners. A key principle of this approach is to differentiate between support of bespoke applications from the support of commodity Software as a Service (SaaS) products because each requires a difference focus. For SaaS products, the principles around APM may apply, but there are less opportunities for automation. The focus for SaaS support is more focused on configuration and business process management.

Bespoke	SaaS
Focus on code, innovation, rapid development, automation, environment control, continuous improvement of functional and non-functional attributes	Focus on integration and business process regression testing, configuration, IAM and Security to accommodate vendor upgrade cycle
Technology driven	Business process driven

High-level requirements for creating automated production environments for bespoke applications are detailed in Table 1.

Table 1, Requirements

ID	THEME	REQUIREMENT HEADLINE	NOTES
1.1	APM	Monitoring of the real user experience - end to end across all transactions	Not sample driven. All transitions for all user for all apps. End to end and top to bottom
1.2	APM	Monitoring at each layer of the production environment making visible the performance and interaction of each component.	A data rich environment is required to create input for AI driven learning and decision making. Initially this will benefit probable root cause analysis - later used for AI driven decision making for self-remediation / capacity management etc
1.3	APM	Performance data from production used by development upstream to target improvement	APM data in production not limited for use by I&O but should be accessible and used throughout application pipeline
1.4	APM	Toolsets operate with open API capabilities supporting innovation is data connection	Value comes from connecting data. The data itself will become of significant internal value to IT and therefore should be accessible to all against which to great new and novel applications
2.1	AI Ops	Probable root cause analysis to expedite fault investigation	Volume of machine-generated data overwhelms manual inspection but suited to AI driven inspection, correlation and suggestion of probably route cause. Human validation and decision making still required after machine driven heavy lifting.
2.2	AI Ops	Deterministic detection of anomalous changes in performance	Negates effort to maintain manual performance parameters which are likely to go stale and trigger false alarms
2.3	AI Ops	Real time topology and performance data for fault analysis - without manual intervention	Future proofing for dynamic environments where impractical to record infrastructure and component dependencies. Requires real time tracking of actual (not assumes) environment / infrastructure configuration
2.4	AI Ops	Accesses severity by known number of impacted users	Linked to monitoring every transition - real time actual report on users transacting with applications for better understanding of impact
3.1	Automation	All tool sets converge at a single orchestration layer	Comprehensive monitoring required best of bread tool selection, but convergence required to drive future automation from a single orchestration layer. Data convergence creates a richer set to find correlating patterns from disparate sources and for machine learning.
3.2	Automation	Applications are deployed with no manual intervention	Sets the standard for Design to Operate principles. Implies standards and ways of working upstream DevOps practice and toolchain. Automation benefits for build, testing and release overlap with the same requirements for I&O
3.3	Automation	Self-remediation built into app design	Preparation for NoOps future enabling application failures to be rectified by automated action from orchestration layer.
4.1	Practice	Design to Operate principles are strictly applied to qualify applications to run in this environment	An automated environment will require compliance to be engineered in from the start. The DevOps toolchain will be in effect the design filter because it will mirror production requirements.
4.1	Practice	New releases are baselined against existing operational performance data, so they are proven before deployment	Part of the test regime expect pre-production to guard against retrograde performance upgrades. Updates should have proven benefit

Digital IT Operations – Infrastructure and operations

The Infrastructure and Operations (I&O) area of IT plays a critical role as part of IT Operations, overseeing IT infrastructure and Service Management, Solution Delivery and Governance across End User devices and services, Network Connectivity and Compute platforms including SaaS, PaaS, and IaaS cloud based solutions supporting National Grid's business and customers.

We will invest on process improvements and tools delivered to all critical I&O functions:

- **Operations Management and Governance** - Opportunities to deliver improvements in this space will focus on extending the key pillars of our RIIO-T2 strategy, which consider capability areas around people, process, technology and data.

  I&O will also focus on maintaining our asset health policy to improve performance, reduce risk and deliver the greater value to internal and external customers of our IT infrastructure.

  The use of common platforms, rationalizing how infrastructure and applications are deployed and consumed will reduce overlap and costs to support our purpose to Bring Energy to Life.

- **Availability and Capacity Management** - The use of new tools combined with process improvement, automation, and analytics will deliver a deeper understanding of our IT services and infrastructure consumption, providing a predictive forecast to identify when and where we need to deliver capacity.

- **Asset Management** - The large and dynamic nature of the National Grid IT estate creates specific challenges in maintaining an accurate view of the assets and software packages deployed. One of the key requirements in digitising IT operations and extracting the benefits of AI and automation is tracking the configuration of the IT estate.

  Investing in infrastructure discovery tools will deliver a granular view of our infrastructure inventory, enabling our CMDB (Configuration Item Management Database) to correlate infrastructure, applications and services, reducing the efforts to maintain the information and ensure it is made available to other key tasks to be completed saving time and reducing costs.

  The delivery of frictionless workflows to support change management and the orchestration of automated workflows associated with customers requesting new technology and applications are a vital component to drive operational efficiency and improved customer experience.

  IT service management tools are vital for the I&O team to deliver IT services in a frictionless and cost-effective manner. ServiceNow is National Grid's platform of choice for the provision of digitised workflows that will enhance the IT value chain, allowing IT to align to the business priorities with speed and agility, delivering AI powered user experiences whilst reducing operational costs.

- **Change Management** - As a critical function to maintain or deliver new infrastructure, change management needs to reach a maturity level where automation and standard changes reduce the time to deliver infrastructure improvements while reducing the risk or failures. The CMBD will play a key role in documenting the relationship between infrastructure, applications and services that will enable the automated risk evaluation, service testing, and validation.

- **Service Desk** – With the right management tools in place, the need to maintain a large service desk footprint will be reduced, relying on bots and pre-defined or automated steps to remotely apply configuration changes or fixes to software and applications.

- **Incident and Problem Management** – Limited end to end visibility at the service layer is preventing I&O from reducing the number of incidents and increasing the time to repair. The combination of Application or Service Performance Monitoring tools and automated CMDB discovery can improve visibility and automate problem detection and resolution via predictive models built from standard performance KPIs and pre-defined baselines for each service or application.

Digital IT Operations – Fault Diagnostics & Resolution

Automation allows for more rapid diagnostics of faults, and over time automation of fixes to resolve faults.

The following cases illustrate time lost in fault diagnosis during an incident. Current practice relies on manual investigation often by multiple suppliers – which can be a significant portion of the total recovery activity. Time from initial impact to diagnosis of the fault accounted for an average 54% of total impact time in the two cases illustrated.

In each case the incident is split into three consecutive phases of the recovery: Impact to Diagnosis, Diagnosis to Fix and Fix to Confirmed Restore. A review of the incident log is used to approximate the time spend (hours) in each phase. This is then compared to how the incident is likely to have progressed if APM was in place with sufficient root cause analysis to cut the diagnosis phase down to just one hour. The actual (No APM) and theoretic (With APM) are illustrated side by side.

Case 1 - US Ops – NRG/QWS & Fortis Citrix – Outage - INC4074868

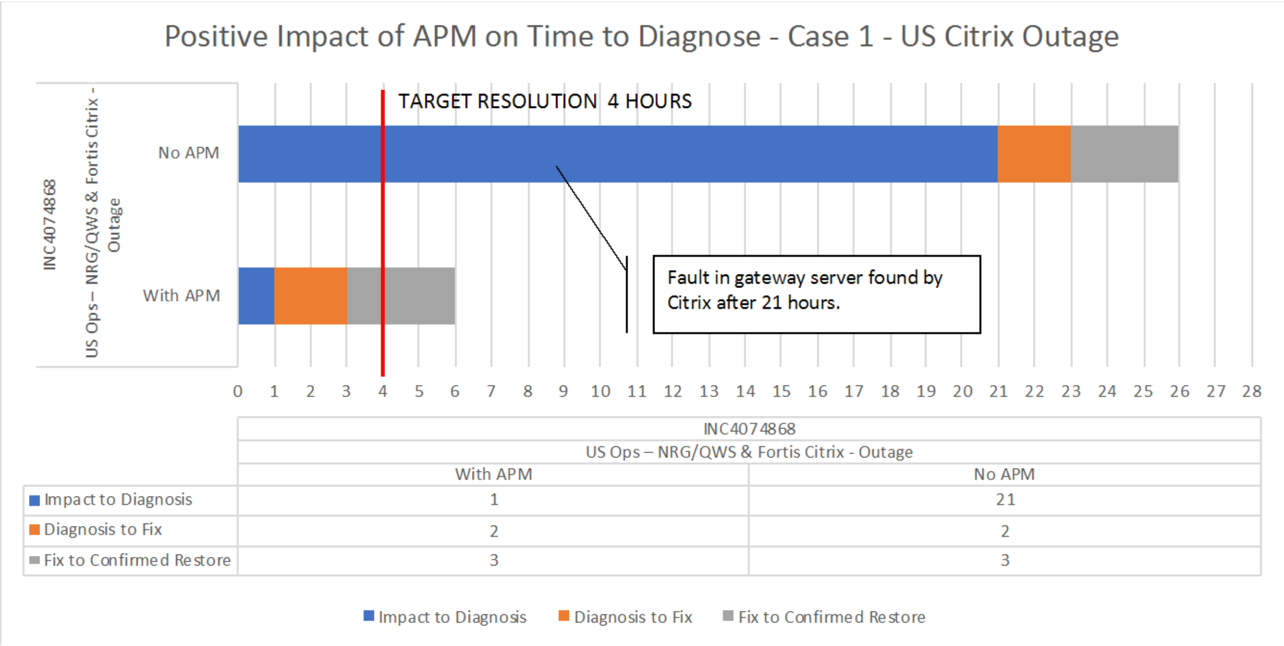
Synopsis of the incident

Citrix Web Portal applications fail to load without any error message. Traceroute implemented and suspect server removed from Citrix farm, but results are inconclusive. Escalated to 4th line support, Citrix who after 21 elapsed hours identified a fault in a Secure Gateway server.

Without Automation	With Automation
Actual impact duration – 26 hours	Estimated impact duration with APM – 6 hours

How would APM have helped?

End-to-end monitoring of user transactions could have identified the presence and cause of each failed transactions in real-time.



	INC4074868	
	US Ops – NRG/QWS & Fortis Citrix - Outage	
	With APM	No APM
🟦 Impact to Diagnosis	1	21
🟧 Diagnosis to Fix	2	2
▨ Fix to Confirmed Restore	3	3

Case 2 – UK Enterprise Content Management application

Synopsis of the incident (Incident Number: INC3466583)

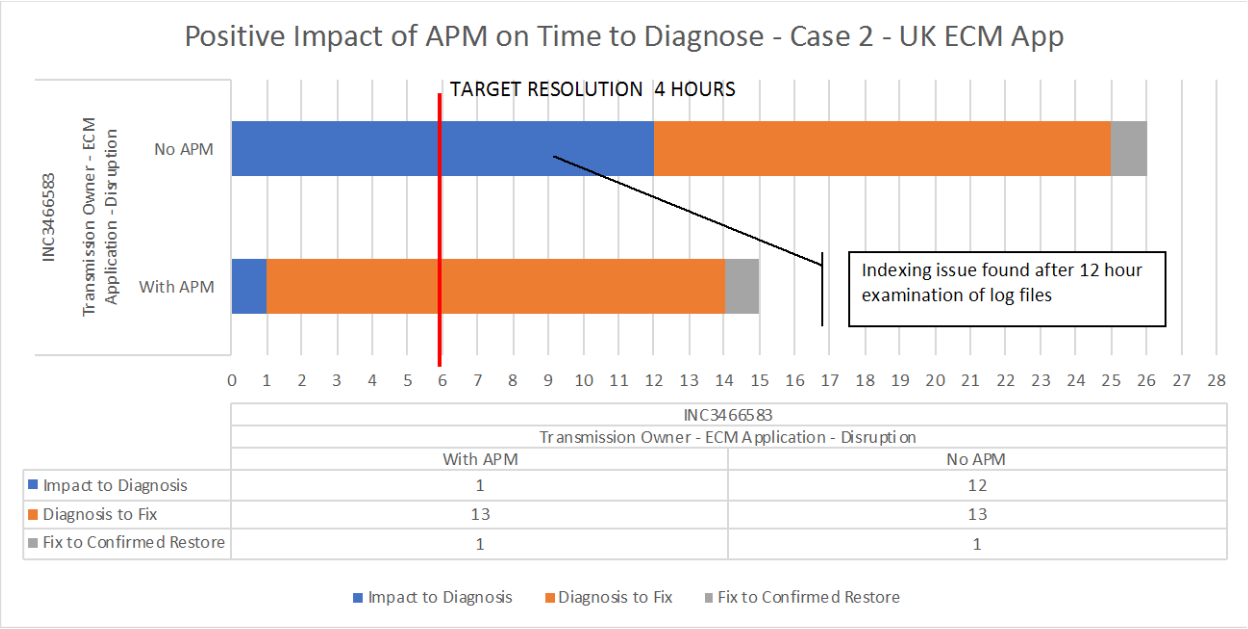
Users were unable to access the search functionality within Enterprise Content Management (ECM) system, leading to potential Health and Safety impact for National Grid. IBM support identified 25% of the search functionality within ECM was unavailable. OpenText diagnosed corruption in 1 of 4 partitions. Restored by re-indexing.

Business Impact

Without Automation	With Automation
Actual impact duration – 18 hours	Estimated impact duration with APM – 7 hours

How would APM have helped?

APM could have identified indexing corruption enabling the re-indexing process (13 hours) to begin earlier.



	INC3466583	
	Transmission Owner - ECM Application - Disruption	
	With APM	No APM
🟦 Impact to Diagnosis	1	12
🟧 Diagnosis to Fix	13	13
⬜ Fix to Confirmed Restore	1	1

- **Technology Roadmap and Release Management** – As part of our proposed plan to maintain a healthy and up to date environment, I&O will utilize automated CMDB discovery tools to track hardware and software inventory to plan and deliver the necessary updates to the infrastructure. Automated patch management utilizing AI validated releases will improve update cycles to reduce operational and security risks.

- **Performance Measurement** - Developing a baseline for infrastructure, applications and service performance using tools and machine learning to measure and predict performance issues before users report problems will allow I&O to track End User experience and reduce the number of incidents.

- **Application Performance Monitoring** - Allows IT to measure the real user experience of an IT application in terms of its availability and responsiveness. Historically when performance degrades the first alert is generally the users calling the Service Desk. As a consequence, the user experience can suffer for prolonged periods while IT reactively addresses the issue.

- **Cost and Operational Budget Management** – The use of cost management tools like Apptio in combination with automated infrastructure inventory and CMDB discovery, integrated to SAP and billing management, and linkage into our strategic planning tools will allow I&O and IT Finance teams to improve the visibility and track cost allocation and performance against the targets, identifying deviations or saving opportunities.

- **Service Catalogue** – Investing more on delivery of standard services and solutions will improve our time to deploy and reduce costs via automated workflows and change management. It is important that we revisit our Service Catalogue taxonomy. The taxonomy and governance of it is critical to delivering a rational, frictionless end user experience.

- **Disaster Recovery and Business Continuity** – Disaster recovery is an area of IT and Security planning that protects National Grid from the effects of a significant negative event maintaining or allowing the quick resumption of mission critical functions. National Grid creates and manages large volumes of electronic data, much of which is essential to the normal operations of the business. While every effort is made in the design of IT solutions to prevent outages impacting users, it is not practicable to engineer full resilience to every system.

  As the technology deployed within the IT estate changes with the increased adoption of cloud compute, using new network and storage technologies, it is necessary to continually update and test business continuity and disaster recovery plans. Standard infrastructure solutions will enable I&O to deliver the required availability at a reduced cost, relying on Digital Twins to deliver the level of assurance required to ensure business continuity in case of a major disaster.

- **Supporting Tools –** Within the Digitised IT operational environment, utilisation of frictionless workflows to support change management, and delivery of automated workflows to support customers requesting new technology and applications are a vital component of driving operational efficiency and improved customer experience.

  IT service management tools are vital for the Infrastructure and Operations team to deliver IT services in a frictionless and cost-effective manner. ServiceNow is National Grid's platform of choice for the provision of digitised workflows that will enhance the IT value chain, allowing IT to align to the business priorities with speed and agility, delivering AI powered user experiences whilst reducing operational costs.

  At National Grid, we adopted ServiceNow during the RIIO T1 period, consolidating our IT service management systems and processes that were previously spread across multiple platforms and offline spreadsheets and generating vital data, analytics and reporting capabilities required to drive the function forward and improve efficiency.

  During the RIIO T2 period we will build on the foundations created, extending the functionality of our ServiceNow platform to include CMDB which in conjunction with Apptio will deliver real transparency to the IT cost base enabling effective decision making and driving ever greater efficiency within the portfolio.

  Core to efficient and effective IT Service Management is a robust, reliable CMDB. Improved CMDB data stewardship and management as part of the digitisation of IT operations will contribute to a reduction in service outages and enable faster incident resolution.

  The more we ask of the ServiceNow platform, the more critical the CMDB becomes. For example, Security Operations may consider using ServiceNow for Security Incident Response or Vulnerability Detection and Response. A dated, manual discovery mechanism that doesn't have sufficient coverage of Configuration Items on our networks, would reduce the value of investing in that functionality without an approach to improve the underlying data.

  ServiceNow's business model is to provide wide ranging native functionality, while realizing they usually won't be the preferred option for all "business of IT" functionality. Therefore, they have a robust integration approach that includes an Integration Hub, a well-defined and mature API strategy as well as hundreds of prebuilt integrations available via the ServiceNow Application Store. These mechanisms allow ServiceNow to interface directly to other key business and IT services, linking to Identity access management (IAM), Success Factors (HR system), SAP and Infoblox (IP address management), and Technopedia (normalisation and market intelligence) allowing the creation of frictionless digital workflows across a wide range of Business and IT services improving efficiency of the enterprise.

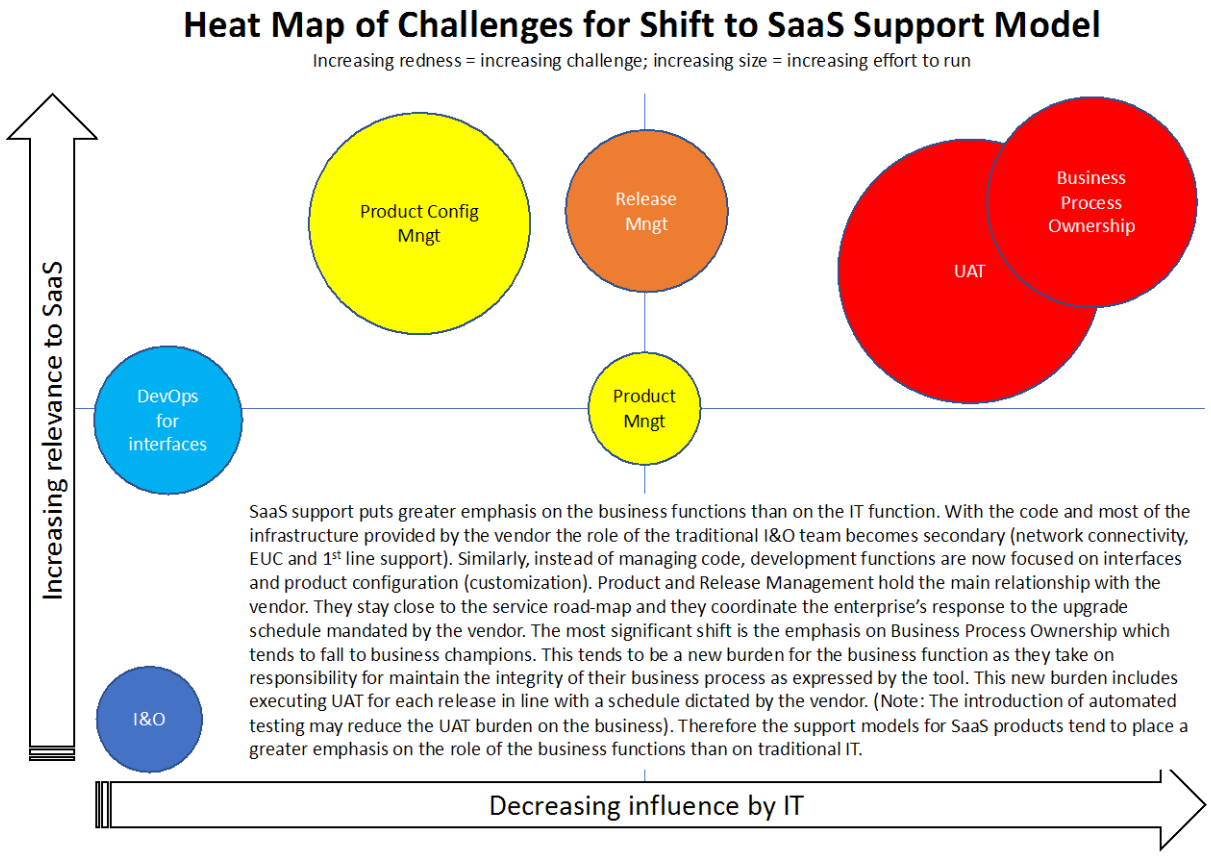
ServiceNow is a constantly developing platform with incremental capabilities being released in twice yearly updates. Some of that functionality is included in our existing contracts, but others require additional investment. Examples:

- Governance, Risk & Compliance modules are included in our existing entitlements
- AI, Machine Learning and Natural Language processing require additional investments

- **SaaS Support -** For the support for SaaS products, the emphasis is placed on business functions and their new role in maintaining how business processes are expressed by the tool. Traditional IT, and hence the role of I&O is relegated to ensuring the basics of network connectivity, EUC and Support Desk functions are in place.

  Opportunities for automation do exist, for instance, in automated User Acceptance Testing (UAT) of business process, or in automating monitoring and incident management processes. But the opportunities are less than is the case for the portfolio of bespoke applications developed by and on behalf of National Grid.

  The figure below illustrates how the key considerations for supporting SaaS products tend to fall to the business functions, as represented by the top right quadrant.



Heat Map of Challenges for Shift to SaaS Support Model

Increasing redness = increasing challenge; increasing size = increasing effort to run

Product Config Mngt
Release Mngt
Business Process Ownership
UAT
DevOps for interfaces
Product Mngt
I&O
Increasing relevance to SaaS
Decreasing influence by IT

SaaS support puts greater emphasis on the business functions than on the IT function. With the code and most of the infrastructure provided by the vendor the role of the traditional I&O team becomes secondary (network connectivity, EUC and 1st line support). Similarly, instead of managing code, development functions are now focused on interfaces and product configuration (customization). Product and Release Management hold the main relationship with the vendor. They stay close to the service road-map and they coordinate the enterprise's response to the upgrade schedule mandated by the vendor. The most significant shift is the emphasis on Business Process Ownership which tends to fall to business champions. This tends to be a new burden for the business function as they take on responsibility for maintain the integrity of their business process as expressed by the tool. This new burden includes executing UAT for each release in line with a schedule dictated by the vendor. (Note: The introduction of automated testing may reduce the UAT burden on the business). Therefore the support models for SaaS products tend to place a greater emphasis on the role of the business functions than on traditional IT.

Digital IT Operations - Security Operations

Attack surfaces and risk profiles within cyber security can change quickly; we need to enable both our IT and Security Operations to respond at speed to those changes, to ensure National Grid's cyber posture continuously improves. Our approach to delivery of Security Operations aligns closely with the DevOps culture and automation recommended throughout this paper.

There are two aspects of automation that Security Operations will adopt:

1. The delivery of products and solutions into the Security Operations to be consumed by Security Operations, or by the wider National Grid businesses.
2. The delivery of service by Security Operations.

Delivery of Products and Solutions

The delivery of Security capabilities is split into the following capability pillars:

- Vulnerability Management
- Identity & Access Management

- Response & Recovery Planning
- Security Operations (Security Operations Centre; Response; Forensics; Recovery)
- Network Security
- Platform Security
- Data Protection
- Awareness & Training
- Third Party Management
- Cyber Risk Framework
- Performance, Threat & Specialist Services

Each pillar has the responsibility to identify, develop, deliver and operate products and services within their remit (in collaboration with each other, and the wider IT Operations landscape). The ways of working being adopted is not dissimilar to a DevOps model, that will mature during RIIO-T2. As our Security Operations progress on their journey, automation will be identified in an appropriate DevOps tool-chain to improve delivery cadence and/or reduce delivery costs.

Adoption of Continuous Integration and Continuous Delivery techniques; and tooling for automated security testing, are examples of where we will aim to improve our delivery capability.

Delivery of Service

Automation is a key cornerstone to the success of delivering security services to any large organisation. The variety, volume and velocity of data being received by these services would impact their accuracy and timeliness if a degree of automation is not achieved.

The following components will provide automation, or will have a significant degree of automation, within Security Operations:

- SOAR (Security Orchestration and Automated Response)
- Big data analytics (example use case is for anomalous behaviour detection)
- Vulnerability detection and remediation (automated workflows)
- Intrusion detection (raising of anomalous events)
- Continuous threat assessment

External Compliance

Our Security Operations and their services are being delivered in line with the NIS regulations legislation that came into force in May 2018. We have followed the NCSC Cyber Assessment Framework (CAF) self-assessment, which has driven our immediate (RIIO-T1) and RIIO-T2 cyber posture improvement plans.

Our improvement plans have been drawn up with close engagement of both the NIS Competent Authority and Ofgem.

Please refer to the RIIO-T2 Business IT Security Plan for more detail.

Digital IT Operations – Application Performance Monitoring and Maintenance

APM allows IT to understand the real user experience of an IT application in terms of its availability and responsiveness. Historically when performance degrades the first alert is generally the users calling the Service Desk. As a consequence, the user experience can suffer for prolonged periods without IT being aware there is an issue.

What's the problem with the Current approach to application maintenance?

Currently IT Operations has limited real-time data on end-to-end application performance, technology interdependence or user experience. In some cases, system health checks are performed manually on a daily or hourly basis. At best pockets of performance data exist but lack connection to other data sources, making correlated insights an impossibility.

Fault diagnosis is a common inefficiency. Time is wasted waiting for suppliers to manually extract and then sifting through system logs to identify failures. This process is repeated multiple times as each supplier examines their portion of the technology stack.

Automation and heuristic learning of AI depend on inputs of accurate and rich data. A prerequisite for automation is to create a data rich production environment by applying APM to monitor performance of all transactions at all layers of the software and infrastructure stack. Exposing this data enables AI driven heuristic learning to drive probable root cause analysis (reduced down time – improved user experience) and when fed into an orchestration layer becomes the enabler for automated management and recovery.

At present the production environment monitoring is disjointed and incomplete. The data is neither rich, nor connected. Hence why root cause analysis is a manual and time-consuming task. Where implemented APM is retro fitted and incomplete, so of limited value. To extract maximum value systems need to be designed for APM with the aim of exposing rich data on performance.

Where monitoring does expose performance data the opportunity to act on it is limited because the system has not been designed for automated self-healing and other opportunities that new tooling may afford. Self-healing is a long-term goal and would not be expected in the current production, but that should not preclude designing it into the next generation of bespoke systems.

Designing in automation and monitoring from the start overcomes these problems as it enables the production environment to create rich application performance data insights to drive AI learning and latterly automation via orchestration tools.

Why can't we just improve what we have?

Automation, performance monitoring and artificial intelligence present opportunities which were previously out of reach. Gartner describes AI for IT Operations (AIOps) Platforms as emerging but predicted to be transformational in 5 to 10 years, leading to: agility and productivity gains, service improvement and cost reduction, and mitigation of risk. (Gartner - Hype Cycle for I&O Automation, 2019).

10X improvements may be possible but only if applications are designed to leverage these tools. Retrofitting IT Operations tools as an after-thought will not be sufficient to achieve these gains.

For this reason, incrementally improving the current approach will not suffice. A comprehensive “Design to Operate” policy is required to ensure the benefits of new technology can be fully exploited. Automation has to be built in from the start.

> ‘Automation is no longer optional. It is a response to the increasing complexity and scale of next-generation technologies. Those problems can’t be solved without it.’ (Gartner – Solution Path for Infrastructure Automation – 2019)

This is a step-change in approach where the needs of the production environment mandate how applications are designed upfront. Doing so unlocks benefits throughout the software lifecycle as development cycle times are reduced and IT resources focused on outward value-add activity.

The implications flow upstream into the build and design stages of the lifecycle. Automation in IT Ops is an extension of the DevOps pipeline with overlapping aims and outcomes. According to Gartner ‘The "continuous" integration, testing and delivery paradigm, now commonly leveraged by agile product teams, offers similar benefits for I&O automation teams’ (Gartner - To Automate Your Automation, Apply Agile Practices and DevOps Tools to Infrastructure and Operations – 2018).

The paradigm shift is to take DevOps principle of agility via automation and extend it into the IT Operations framework.

What are the guiding principles of this strategy?

Guiding principles shape coherent action to support the strategy.

- Bespoke IT solutions are designed to be deployed and operate without manual intervention
- Performance monitoring is end-to-end and top-to-bottom, there are no boundaries (including the user experience for all transactions for all users all the time)
- Tools supporting the environment are best of bread but are integrated to a single orchestration layer from which actions can be automated
- Intelligent operations tools use AI and machine learning to detect out-of-bound performance and suggest root causes of failure
- Design to Operate principles are strictly applied to qualify applications to run in this environment
- System improvements are driven by performance data insight, so changes are targeted and efficient
- New releases are baselined against existing operational performance data, so they are proven before deployment
- Automation is used throughout the build and test process allowing nightly build and test cycles
- A modular build approach combined with short development cycles and continuous and automated build / test enables IT to confidently and flexibly adapt solutions to support new business opportunities
- Software is built and tested against the same APM tools as used in the production environment
- All supplier / partners have visibility of the production environment performance data which is regarded as the source of truth

What is the pathway to implementation?

Implementation is staged in phases, each with increasing scope as capital in automation is built over time.

Short term (0-2 years) – surface the data

Implement end-to-end and top-to-bottom APM across the existing production environment where compatible. This includes user experience monitoring, automated inventory management, and full software / infrastructure stack performance monitoring. The outcome is to gain control of the environment, reduce MTTR, increase uptime and enhance the user experience. All partners rely on a single source of truth. Experience of creating rich data insights will be used design the next generation of IT solutions and architectural choices. This is how and where the Design to Operate mandate is forged.

Prove Design to Operate with small scale (low risk) implementation of Digital Prototypes built to the new automated standards. Prove what works, refine what doesn't ahead of major commitment in the next phase. Start small to unlock value *["Fire bullets first, then cannon balls" – Jim Collins*].

Medium term (2-5 years) - repurpose applications

The application portfolio is being refreshed through reinvestment. Generic services are provided by vendor platforms, bespoke solutions are designed accorded to the mandated Design to Operate principles, which are now fully verifiable in the test environment. A solution is not released until it is validated. Solutions are modular, frequently iterated and rely on automation for deployment and operation. Solution design begins and ends with the user experience and operational performance data. Over 80% of events are fixed without manual intervention. Average MTTR is reduced from 5 hours to 30 mins (a 10x improvement). Application Maintenance costs are reduced enabling more resources to be directed to developing new solutions to support the business. Increasingly Development and Operations teams merge. The short development and release cycles increasingly need operational input to manage. DevOps teams arise to support this rapid development cycle.

Long term (5 years plus) – remove IT Operations

AI and orchestration have enabled applications and infrastructure to run with minimal manual intervention, delivering significant reduction in operational cost.

Digital IT Operations – Discovery Tooling

As the rate of change increases across the IT landscape through increased automation as described in this paper then the need for automated discovery tooling also increases. Automated discovery tooling enables information to be collected on services, hardware and software in real time ensuring information is up to date in a rapidly changing environment. This is required to address several key areas:

- Software and service license compliance: An accurate inventory of software and services used and their licensing usage is critical to ensure there we remain compliant with the terms of our licensing agreements.
- Cost management: To maintain an accurate cost of services is key to decision making and cost transparency. This will enable National Grid to operate services most efficiently to meet customer demand
- Configuration Management: Accurate configuration management information is critical for problem and incident resolution and change management to ensure that any planned or

unplanned changes have the desired effect on the services being impacted. Out of date information can lead to intervention errors and inadvertent loss of service

6 Strategic Platform Investment areas

Demand, portfolio, project and architecture management

Aligning business strategy and demand to change initiatives and the underlying architecture is critical to managing change most efficiently and cost effectively and delivering the strategic intent of the organization. A consolidated platform or set of integrated products will ensure alignment and visibility across the whole planning and execution lifecycle and is a cornerstone of the effective management of the business of IT. In T1 investments have been made to maintain and integrate point solutions but this will need to improve and increase throughout the T2 regulatory period in order to support the increasing demand and speed of change and optimise the delivery of T2 investments.

Disaster Recovery

Disaster recovery is an area of IT and Security planning that protects National Grid from the effects of a significant negative event maintaining or allowing the quick resumption of mission critical functions. National Grid creates and manages large volumes of electronic data, much of which is essential to the normal operations of the business. While every effort is made in the design of IT solutions to prevent outages impacting users, it is not practicable to engineer full resilience to every system.

As the technology deployed within the IT estate changes with the increased adoption of cloud compute, new network and storage technologies it is necessary to continually update and test business continuity and disaster recovery plans.

Discovery Tooling

The large and dynamic nature of the National Grid IT estate creates specific challenges in maintaining an accurate view of the assets and software packages deployed. One of the key requirements in digitising IT operations and extracting the benefits of AI and automation is tracking the configuration of the IT estate. A CMDB continually monitored, updated and verified by discovery tooling plays a vital part on the digitisation journey.

ServiceNow

Within the Digitised IT operational environment frictionless workflows to support change management, and orchestrate the automated workflows associated with customers requesting new technology and applications are a vital component of driving operational efficiency and improved customer experience.

The ServiceNow platform is National Grids platform of choice for the provision of digitised workflows transforming the IT value chain allowing IT to align to the business priorities with speed and agility, delivering AI powered user experiences whilst reducing operational costs. IT service management tools are vital for the Infrastructure and operations team to deliver IT services in a frictionless and cost-effective manner.

At National Grid, we adopted ServiceNow during the RIIO T1 period, consolidating our IT service management systems and processes that were previously spread across multiple platforms and offline spreadsheets and started to generate the vital data, analytics and reporting capabilities required to drive the function forward and improve efficiency.

During the RIIO T2 period we will build upon the foundations created, extending the functionality of our Service Now platform to include CMDB which in conjunction with APPTIO will deliver real transparency to the IT cost base enabling effective decision making and driving ever greater efficiency within the portfolio.

Core to efficient and effective IT Service Management is a robust, reliable CMDB. Improved CMDB data stewardship and management as part of the digitisation of IT operations will contribute to a reduction in service outages and enable faster incident resolution.

Software asset management provides the ability to set up license abstracts, implement automated license re-harvesting and act upon various license thresholds. To derive maximum value in software asset management, we will need to invest in the ServiceNow Software Asset Management module. This functionality enables transparency and reporting to become near real time and avoids requiring projects each time we to accurately identify overlaps in an increasingly complex licensing model, this allows us to monitor and rationalise our technology estate in real time without months of analysis and large project teams.

Service Now additionally allows IT to interface directly to other key business services, linking to Identity access management (IAM), Success factors (HR system) and SAP allowing the creation of frictionless digital workflows across a wide range of Business services further improving efficiency of the enterprise.

Service now is a constantly developing platform with incremental capabilities being released in twice yearly updates, continued investment is required to ensure that as new capability is added to the platform, maximum benefit is derived from these capabilities.

Infrastructure and Network Operations Centres – iNOC

Within the National Grid IT estate there are multiple network operations centres, each supporting specific assets and providing specific monitoring capabilities. These include the OpTel Network Management Centre, the CNI System Health Team, the Enterprise Network Monitoring Team, the Data Centre Monitoring Team and the Cyber Security Operations Centre. These functions currently operate independently across multiple National Grid and 3rd party locations, each with independent management and reporting lines. These operation centres also reflect the functional responsibilities of each of our strategic service partners.

As the IT estate becomes increasingly digitised, reducing the need for manual intervention in the operation of the IT estate, the standalone nature of the varied NOC capabilities within the estate becomes increasingly inefficient and less effective than it could be if integrated into a single unified Operations Centre.

The network operation centres also have a key role in enabling National Grid to manage the performance of vendors by being able to directly monitor and interrogate the systems, without being dependent on reports provided by the vendors. National Grid's ability to scrutinise asset discovery, network monitoring, application performance monitoring and similar tools plays an important role in validating the performance of vendors and providing quantitative data against which to identify and define improvements.

In bringing all independent NOC capabilities into a single function we drive efficiency by eliminating the multiple management structures required, streamlining to a single line management structure. A single unified NOC will also improve the effectiveness of communication and cooperation between capabilities by bring them together under a single roof and improve the overall National Grid capability by bringing in-house monitoring and reporting on the holistic IT estate.

To illustrate the benefits of a single NOC covering the complete estate, imagine a scenario where a project deployment requires a small change in Network configuration. The configuration change has been through change control and is approved, but due to human error (the most common cause for failure) the change causes the isolation of a range of servers in the data centre, leading a failure of some functionality in an application. In the current model, this failure would potentially be identified by a user who reports and issue with an application, this report would generate a ticket to the application maintenance team. The application management team would diagnose an issue with the servers and need to pass the ticket for resolution to the data centre team, a service provided by a 3rd party provider located on a different site. The Data centre team would in all likelihood confirm that the servers are running normally but the network appeared to be down. This would transfer the ticket to another NOC at another location, before diagnosing that the recent change implemented on the network had caused an issue. The number of handoffs between monitoring capabilities, all add cost and complexity to what could be a simple resolution.

The intent of infrastructure and network monitoring capability is not to function in independent silos, but unfortunately this is what has occurred as the IT function has grown in capability and complexity. As technology becomes more and more ubiquitous in modern workplaces and greater levels of automation are becoming available, now is the time to address the legacy services we operate with today and redefine how of technology will be monitored and managed into the future.

A single iNOC encompassing the monitoring of all technology capabilities, drives improvement in both effectiveness, and efficiency. Failure to address the legacy of historic technology monitoring will perpetuate elevated costs, impair improvement in service, and most critically block the future automation of technology management.

Once enabled with the required infrastructure and tools, the iNOC will deliver end to end visibility across the entire National Grid infrastructure and partners, collect logs and performance data from End User, Cloud and Hosting, and Network devices and the automation to analyse and correlate events that would otherwise require hours of work between National Grid and its infrastructure partners to identify. In addition, the data collected can be retained and used as input to analytics engines which will initiate preventative maintenance tasks and support asset investment planning based on predictive service outages.

7 Optioneering

In reviewing the options to deploy digitised, automated IT operations it became apparent that there is little benefit to be derived in “cherry picking” individual parts of this strategy.

While some small benefits may be achieved in streamlining the management of NOC under a single line management, within a single location, that alone would not deliver the benefit to justify the actions in value for money terms.

The significant benefits available are only fully delivered by delivering automated and digitised operations, where AI and machine learning are deployed to proactively monitor application performance. The reduced dependence on reactive outage investigation and resolution not only deliver considerable benefits to user experience but also deliver substantial operational savings.

Discovery tooling that monitors the configuration and performance of the IT estate feeding CMDB with accurate real time data, enabling effective and accurate cost allocation and control. This transparency of accurate data enables effective decisions on cost levers ensuring that the full implications of investment decisions are understood.

The automation of IT operations is further extended to the provision of new User services through self-service portals that manage the end to end workflows for a fully automated delivery removing friction from the process and improving agility and user experience.

Each of these capabilities are interdependent where removal of one significantly impacts the whole, diluting benefit both in terms of value and experience.

It is therefore considered a binary choice, to perpetuate the current operational model, with-it constraining the operational benefits of new technologies such as cloud services or embrace the future, pivot the operational model to leverage new capabilities and with-it drive value through the operational cost savings available.

Our assessment of the option and a baseline do nothing are provided in the table below. The assessment is carried out against a set of criteria, specifically:

- 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

Table of options considered

Option	Total Cost of Ownership	Capacity to Deliver	Business / Strategic Fit	Addressing the problem	Risk	Overall
Do Nothing – Retain existing levels of automation and manual activities	**Red** While no new cost is incurred, there are avoidable costs incurred which make this option uneconomic	**Green** Use existing skills, resources and contracts.	**Red.** Service disruption as interdependencies and complexity increases.	**Red** Does not address customer experience, resilience or recovery.	**Red** Risk of missing problems owing to the number of stages involved and the mix of manual and automated.	**Red** Baseline is rejected
Option 1: Consolidate NOCs into a single centre and invest in IT tooling	**Green** While investment is necessary, the savings and avoided costs over the longer term make this an attractive option	**Amber** Consolidating NOCs is likely to raise unforeseen problems.	**Green** Facilitating the automation of processes and services is fully aligned with the requirements of our customers and supply chain.	**Green** Addresses the customer experience and allows for greater resilience and recovery.	**Amber** There is risk in consolidating the NOCs, but this can be mitigated.	**Green** Recommended option

8 Detailed Analysis & CBA

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

£m	2022	2023	2024	2025	2026	Total
Preferred Option - Costs	-21.00	-12.00	-8.00	-6.00	-5.00	**-52.00**
Preferred Option - Benefits	5.75	6.80	8.50	7.30	7.30	**35.65**
Net Cost	**-15.25**	**-5.20**	**0.50**	**1.30**	**2.30**	**-16.35**

This investment drives a series of savings and avoided costs including:

- Reductions in required staffing levels and management
- Reduced maintenance costs
- Avoided software costs.

These savings, their quantification and the assumptions underlying them are provided in the associated CBA, and are summarised in the table below for our preferred option, together with 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	-16.50	-16.98	-11.55	-21.44

As can be seen from the tables:

- In the short-term (during T2) the NPVs are negative reflecting the investment costs and the development of the cost savings
- Over the longer-term (into T3) the NPVs become positive as the cost savings continue but the investment costs are finished
- The results are not materially changed under different scenarios such as a higher discount rate or higher/lower costs

On this basis we recommend undertaking the proposed investments in IT operations and tooling.

9 Key Assumptions, Risks and Contingency

- It is assumed that the current engineering and safety constraints will continue to apply throughout the RIIO T3 period.
- Costs and options are based on current available technical solutions. The availability of new or disruptive technology may provide additional technical alternatives at the time of implementation.
- It is assumed that all IT projects are progressed and funded, removal of one or more deliverables may impact the options analysis and cost assumptions associated with the remaining deliverables.
- There is a risk / opportunity that the level of coordination between IT Operations automation and other National Grid IT projects will vary from the levels assumed. Where possible we will leverage projects to deliver efficiencies. with a resultant impact to cost.
- The primary contingency for these proposals will be an increase in staff and manual effort to cater for the increased demand for change across the IT estate, this could be delivered through permanent, contract or IT partners.

10 Dependencies

The operational efficiencies afforded by digitising IT operations and creating a unified operations centre are dependent on the updates to IT technology proposed in Enterprise Networks and Hosting. Without the modernisation of the IT estate proposed it would not be possible to digitise the IT operations sufficiently to enable the AI and automation that enables the savings proposed in this paper. Without the automation delivered by the digital operations proposal we would not be able to deliver the full benefits proposed by unifying out network operations centres.

11 Conclusions

A ‘Digital Business’ opens up whole new business models, and a Digital Transformation agenda applies technology to deliver step changes to address business problems. The same thought leadership can be applied to the internal workings of IT to ensure it has the structural coherence to deliver on its promises.

Automation can unlock 10 times improvements in efficiency and effectiveness, leading to improved user experience, less downtime, more agility and less waste. It can also unlock a virtuous circle of agility and efficiency gains as momentum builds.

Whilst still an emerging field Gartner predicts automation will be “transformative” in a 5-10-year horizon. There is merit therefore in starting to build “automation capital” so National Grid has the skills and experience to exploit the technology fully when it matures.

To unlock these benefits all systems will need to be specifically designed to both be monitored and automated. This will mandate design to operate principles which flow upstream to development and architecture. The alignment of the “pipeline” will itself have benefits because the goals are overlapping.

Doing so will involve a shift in thinking to extend the DevOps principle of continuous build and integration into the realm of IT Operations. Design to Operate principles will shape future systems to be automation ready.

Production environments will need comprehensive APM capabilities so performance at all levels is exposed. Once fed into an orchestration layer this data can drive AI engines for heuristic learning (probably root cause analysis) and latterly automated management of software and systems.

The implementation path begins with early Digital Agenda pilots to prove the principles and develop the Design to Operate mandate (“first fire bullets”). Then, applying the approach to the next round of portfolio reinvestment to scale up (“then fire cannonballs”). Once sufficient automation capital has been amassed the transformation of IT Operations, and other IT processes, can begin.

12 Outputs included in RIIO T1 Plans

Nil