National Audit Office

NAO DIGITAL PLAN 2020 - 2022
Version 2
July 2020

Issue No: 1
Issue Date: 17 July 2020

Document History

Issue Date	Version No	Produced By	Contents
12 June 2020	0.1	A Waugh	First pass iteration from version 1
15 June 2020	0.15	S.40(2)	L&D elements
16 June 2020	0.16	S.40(2)	Comments and context
25 June 2020	0.17	C Hepburn	Updated Financial Audit components
29 June 2020	0.18	S.40(2)	AIMS 1.0 phase 2
30 June 2020	0.19	P Smithson	Updated Financial Audit components
9 July 2020	0.2	A Waugh	Draft iteration version 1.2 (ODP alignment)
13 July 2020	0.25	Y Gallagher	Digital context
15 July 2020	0.5	A Waugh	Draft iteration version 1.3 (costs, roadmap)
17 July 2020	1.0	A Waugh	Final Draft

Final Version Distributed to:

Name	Role
Executive Team	Approval
NAO Board	Comment

Reviewers

Name	Date	Role
D Lambauer	13 July 2020	Executive Director, Strategy & Resources (Sponsor)
G Davies	17 July 2020	Comptroller & Auditor General review
Executive Team	22 July 2020	Executive review
NAO Board	30 July 2020	Non-Executive review

Digital Plan 2020-22 v2

Table of Contents

Executive summary

1   This NAO Digital Plan 2020-2022 (v2 – July 2020) updates the previous version (v1), published in October 2019. Through the NAO Digital Plan 2020-2022 (v2), our vision is to offer a secure and well-integrated digital environment which enables the NAO to deliver its strategic objectives. Since October 2019, we have delivered:

- An Audit Information Management system (AIMS) & new application
- A full migration of all NAO telephony in to cloud provision & refresh of all NAO mobile and desk phones
- ISO27001 certification
- Various upgrades and enhancements to all our content management systems
- Additional cloud migrations taking us to 80% of the corporate estate
- Extended remote working services (in response to COVID-19) including equipment portals, a range of conferencing solutions and connectivity bandwidth increases

2   The updated plan comprises three core pillars: **digital audit, digital workplace,** and **people & knowledge**. This third pillar has been updated to reflect our Organisational Development Plan (ODP, June 2020), all three pillars have been revised to underpin the commitment and actions made in the ODP, providing more detail on the digital elements. The Digital Plan is supported by key guiding principles – that all digital services must be; secure, simple & agile, user-oriented and of long-term value.

3   We continue our journey to migrate all NAO digital services in to secure cloud provision by 2021. In 2020, COVID-19 has impacted all organisations. Within the NAO our investments in cloud services and remote working technologies has enabled us to swiftly respond and adapt to extended home working, minimising the impact on our people and increasing organisational resilience. Having mobile productivity and communications technology has also enabled audit teams to establish that processes previously thought only possible at client sites can in fact be performed remotely (for example laying reports, analysis accounting sheets and signing accounts).

4   Extended home working has also shown that there is still much to do – better connectivity, improved conferencing and collaboration services, enhanced cyber security models, new ways of working across service lines, adapting the digital support operating model, remote onboarding and offboarding and improved digital learning. We have therefore updated our core pillars, re-prioritised key activities within each one and stress-tested all of our plans to ensure that we are equipping the NAO, in the best and safest way, to be an online organisation should we need to build on the associated capabilities and pathways. Certain projects which were planned for later in 2020/21 have therefore been brought forward and others have slipped to later in the plan.

5   This update reflects all the digital work packages within the ODP which sets out the changes we will make to achieve our strategy. The main initiatives reside within the Data & Technology elements of the NAO Strategy, fresh thinking around our people and knowledge is sufficient to comprise a new core pillar within the Digital Plan. More detail on all work packages and deliverables can be found within the NAO Organisational Development Plan. The Digital

Audit core pillar has also been updated to reflect the introduction of the Audit Transformation Programme (ATP).

6   The NAO Digital Plan 2020-2022 is iterative, allowing for priority changes and directional influences which will arise during its lifetime. We have also invited an external review of the plan, comments from which have been incorporated into this version. The next scheduled review will follow in early 2021.

7   An overview Technology Roadmap is at <u>Annex F</u> – this provides a visual representation of the technology capabilities which will be introduced during the lifetime of the plan, together with deployment risk and value to the NAO. A table of deliverables is at <u>Annex E</u>. This table will be updated as part of each update.

Strategic context

8   The strategic case for investment in digital remains the same but has been put into sharper relief with COVID-19. Technology continues to play a key role in the delivery of public services but now even more so for extended remote working and remote communications. We have had to adapt our systems, services, processes, and equipment provided to minimise the impact on the NAO and our people. Specifically, around extended remote working and doing all we can to minimise organisational impact.

9   Integration of technology in the core operation and management of services and far reaching utilising of cloud platforms continues at pace across government. Our ambitious cloud program has paid dividends in exploiting appropriate cloud capabilities and ensuring that we provide high value cloud services to the NAO which we are now seeing our clients adopt. This move to cloud has also positioned us well in needing to operate remotely from our systems and data.

10   These trends continue to affect us in the NAO in various ways. Most directly there is the impact on our own internal business operations, how we manage ourselves and assist our people in the use of the technology provided. We must ensure that we are helping our people make the best use of the technology we provide. The People & Knowledge elements of the ODP direct us to do more to identify and develop the digital competencies that our people need and to nurture and curate the knowledge we possess. The need for greater digital expertise across the NAO is vital to appreciate what government is aiming for digitally and to comment on how and whether success is likely.

11   These implications for the NAO are linked. Our greatest opportunity to add value to our clients is to show that we have grappled with these trends in our own work. And our ability to change the way we audit our clients drives many of the organisational choices we make about our own systems and processes. And so, this digital plan considers how the NAO aims to use technology not just as a support to our wider work, but as a central part of how we plan to adapt to new opportunities and challenges in our external environment.

12   This Digital Plan replaces the Digital Plan 2020-22 v1. While it has a three-year strategic horizon, the plan will be reviewed and developed at least annually as the strategic context and technologies in play change rapidly. We therefore intend to return to the Leadership Team regularly with progress against the plan and iterations where appropriate.

Our vision and guiding principles

Vision

13   Our **vision** continues to be to offer a secure and well-integrated digital environment that enables the NAO and its people to deliver high quality audits, add value to Parliament and our clients, and run its operations efficiently.

14   In an environment where organisations are driven by data and new ways of working, the future of audit is tied to our ability to use and interpret data and make the most out of the information and knowledge we have access to and hold. In the longer term, financial and value for money audits will increasingly rely on: directly accessing client data to analyse transactions, perform new analytical procedures, and to flexibly divert the auditor's activity toward high value-adding activities - improving, for example, the way in which public money and data is acquired, managed and used rather than checking the accuracy of financial records.

15   To achieve this long-term vision, we must ensure that our own approaches support this new way of working. Security and the protection of information is already important to our work; in a data-led world this requirement becomes mission critical. Clients must be able to trust us to access and use data reliably.

16   At the same time, the growing opportunities from new technologies can lead to ever more complicated systems and processes. We must be able to move quickly to adopt emerging best practice, but not so quickly that we build in every new app and fashion. Our overall approach must therefore be one of an innovative adopter of proven technologies, taking note from our unique position of having visibility across the government digital estate of what is working well and of that which is not.

Principles

17   We must continue to ensure that our systems are simple and are easily adapted, user-oriented in focusing only on the core requirements of our mission and achieve long term value. Our vision continues to therefore be based on four key **guiding principles** which describe and govern our strategic decisions about the use of technology.

- **Secure.** The C&AG's statutory privileges – including broad rights of access to information, form the foundation of the NAO's role and mission. In the current environment, where cyber security is an ever-evolving risk, our strategy is to ensure that the trust of Parliament and our clients is maintained through managing client information appropriately.

- **Simple & agile.** With many promising technologies being used we must be careful not to adopt too many different solutions at the same time or to lock ourselves into choices. Given our scale – and the risks that organisational complexity inevitably brings – we must ensure that our technology choices are as simple and consistent as possible. We need a simple data & technology architecture which allows us to move with market and technological development. Similarly, adopting agile principles will ensure that services are suitable – utilising delivery methods which allow flexibility in what digital solutions we deliver and how we respond to related threats and opportunities. Strategic, long-term supplier partnerships

can provide value and continuity, we must always ensure that we have an exit strategy which we are in control of.

- **User-oriented.** Our core mission is to help Parliament hold government to account and help ensure public money is spent well to improve public services. Our technology choices must reflect this ultimate purpose and consider the implications for our ability to undertake financial audit and value for money work and fully exploit our cross-office information and knowledge assets. In addition, we will design and implement working practices that optimise the use of technology while designing low level error out of the system, ensuring that risk diminishing decisions can be taken at the lowest possible level.

- **Long term value.** As with all our decisions, we must be able to demonstrate to Parliament that our spending itself represents good long-term value for money. Long term, because with technology choices we must consider not just the standalone choices but also the wider implications for our work, and our wider technical architecture and integration. And sometimes this will mean making tactical decisions – to keep legacy systems running or constructing more temporary solutions to technical problems – where we need time to develop a more strategic option.

18 [Annex A](#) develops these four principles in more detail through our 13 enterprise architecture design principles. In making any decision about what systems and processes to buy, design or build, we aim to adhere to these principles.

The core pillars of our digital plan

19 The principles set out above govern all our strategic decisions. They set the parameters for the strategic choices we need to make. Below we outline the specific strategic choices. We focus these on three pillars that we believe should drive our prioritisation in digital investment. They are closely linked to our vision and the wider ambitions of our NAO strategy. These pillars are; **digital audit, digital workplace** and **people & knowledge**. The pillars operate within a framework of sub-workstreams and work packages which can be found at Annex B, in summary:

Digital Audit	Digital Workplace	People & Knowledge
Modernising Financial Audit • Audit Transformation Programme • IT audit capabilities • Applications & automation	**Content, Collaboration & Continuous Improvement** • Content delivery • Collaboration & conferencing • Continuous improvement	**People** • Development of digital skills & competencies • Improved digital learning • Improved employee experience
Modernising VFM • Modernising VFM production • Software, storage & management	**Technology** • Cloud migrations • Remote working enhancements • Net zero carbon neutral targets	
Audit Information Management • Enhanced data service & analytics • Simplified approach • AIMS 1.0 phase 2	**Information Security** • ISO27001 & continuous assurance • Identify, protect & detect • Respond & recover	**Knowledge** • New Knowledge model • Wider engagement channels • Improved use, re-use and impact

Digital Audit

20 We have an overarching objective to; improve quality, generate greater value and insight, and adopt system-wide audit approaches across all our audit practices. Improvements in digital audit are structured across three workstreams which reflect the two service lines and our management of client data:

- **Modernising Financial Audit** – ensuring our audits evolve to take advantage of new technologies and are managed through effective digital systems.

- **Modernising VFM & Investigations** – improving the way we deliver VFM audit through better use of available technologies

- **Improved Audit Information Management** – delivering a new audit information management system (AIMS) platform to improve quality, generate insight and embed data analytics as standard in our audit work

Modernising Financial Audit

21 The primary component of modernising the way we do Financial Audit is through an audit transformation programme (ATP) and so naturally that is the primary component of this Digital Plan. Below we set out the context for ATP but also recognise that there are three areas where we will continue to develop our digital Financial Audit capability:

(i)   The Audit Transformation Programme (ATP)

(ii)   Continuing to develop our IT audit capabilities

(iii)   Developing business applications which support our FA teams

Audit Transformation Programme

22 The financial audit profession has come under significant scrutiny in recent years in response to several corporate failures where the perception was that the auditors could have done more to signpost the risks of such failures. This scrutiny is evidenced by a wide range of public reviews undertaken to reach a view on how the auditing profession should be reformed such that it can become more effective at holding management to account on the management and stewardship of the organisations and corporations they run.

23 Arising from this has been some key themes including greater audit focus on an effectiveness of organisations' business processes & controls and the greater use of technology in the delivery of the audit. These themes have been a key input into the NAO's current review of its audit methodology so ensuring that NAO's future audit approach will:

(i)   make greater use of reliance on the processes and controls operated by the entities the NAO audits

(ii)   make greater use of technology and data analytics in the execution of the audits.

24 These investments in an enhanced methodology and transformation of the NAO's approach to financial audit delivery has been presented and approved by Parliament and this forms a key component of the updated Digital Plan. Given the strategic importance of this project, the NAO Board will be closely engaged with this part of our digital plan through receiving regular updates on this project and in approving each significant stage of investment.

25 In summary, we have a "Financial Audit Transformation" programme underway, which will make greater use of technology in our audits, and has an overriding objective of ensuring that our approach to financial audit is efficient and high quality, is reflective of the enhanced expectations of the audit profession and is competitive with the commercial sector audit providers (to the extent it is appropriate to do so). Our investments are focussed in the following areas:

- **Enhance quality:** by using automated tools that help our auditors focus and document work on the key risks to their clients and their audits; and workflow tools that enable enhanced in-flight quality activities.

- **Increase client insight:** through ongoing training of our staff to ensure they understand:

    (i)   the technology dependant aspects of the financial business processes of the organisations we audit,

    (ii)   the risks those processes pose to financial reporting, and

    (iii)   understand the audit testing methods and approaches that need to be adopted to test competently the controls that mitigate any financial risks that may arise through technology enabled finance systems. We expect teams to look across whole populations in a data driven way to identify and respond to risk and use that knowledge to add value to stakeholders.

- **Deliver efficiency:** by automating the more routine aspects of our work to allow it to be done more quickly and so ensure we focus effort where in-depth work is needed

26 In line with the financial audit approach as set out in the ODP our audit transformation programme comprises three projects:

- **Audit methodology review –** the overall programme is driven by a review of methodology, representing the most substantial change to how we carry out audits in over a decade.

- **Audit software review** – a comprehensive review of our needs from software tools and a multi-stage process for ensuring that we have the right tools to support and deliver our revised methodology

- **Audit of the future** – assessing the art of the possible for financial audit, maximising the potentials from technology. This includes application development where that best meets audit transformation needs. Consistently capturing and analysing client data to assist assurance and insight.

Audit Transformation Programme scope & alignment
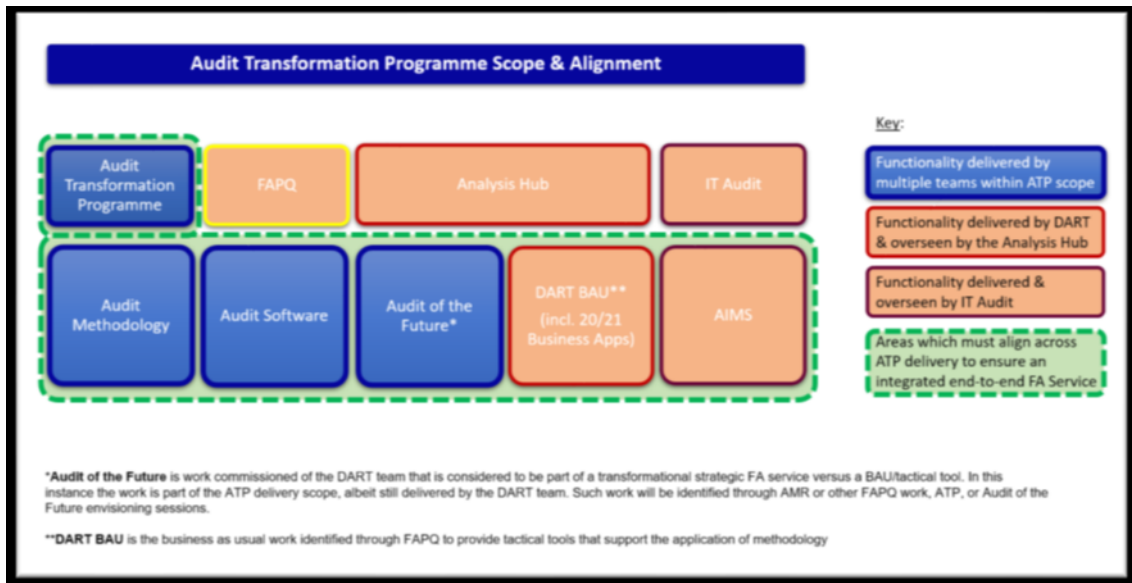
27   Audit methodology review (AMR) – The AMR is driven in part by revised international standards and by wider developments in the profession (see the ATP business case for more details). The outcome will incorporate revised audit workflows to improve compliance and quality, removal of the 50% substantive assurance threshold and qualitative, rather than quantitative, assurance models. These will lead to new ways of working for our audit teams and a different set of demands placed on the supporting software.

> **Digital Plan deliverable (DA01)** – The ATP will produce scenarios where a revised approach to Financial Audit interfaces with supporting software tools

28   Audit software review (ASR) – The ASR project will consider how the NAO's financial audit management/audit documentation tools need to evolve to provide the technology required to support the NAO's plans for financial audit. Within the lifespan of this Digital Plan the NAO will introduce improved audit management, control and automation software which more closely aligns with our new methodologies. To support the AMR the ASR project will:

- Determine the most appropriate tool in the market to support the NAO's future financial audit needs,

- Invest in the design and implementation of a revised solution

- Roll out the revised system to the wider office, ensuring adoption through engagement and learning

> **Digital Plan deliverable (DA02)** – The ATP will identify revised technology requirements, establish the best technology solution components to meet those requirements and implement a revised technology toolset for the 2022/23 audit cycle.

IT Audit capabilities

29   The bodies we audit are increasingly seeking to automate their processes, such that their end to end processes, and related controls are increasingly automated and so reliant on IT

systems. We have an ongoing programme of training and staff skills development to build, and then maintain the skill levels of our NAO audit teams in auditing the IT enabled systems (often complex systems) that our clients operate. The greater focus on an audit approach that seeks to rely on controls (rather than detailed testing of transactions) allows us to meet our clients increasing expectation of us to have a view on the efficiency and effectiveness of their finance business systems, as well as an expectation that we will rely on these management controls to the extent that it is possible to do so.

30 Our new Digital Hub will be key to increasing digital expertise and understanding and to provide deeper insight on how failing systems and projects affect wider areas covered by our revised methodology. The Hub will help the office to become more digitally literate and increase our IT audit capacity and capabilities. See below for further details on the Digital Hub.

Applications and automation

31 The ATP focuses on the broader transformation of the Financial Audit service line. Alongside this we will continue to develop and implement applications and automations to improve the efficiency and accuracy of audits. Building on the AIMS platform, these applications will apply consistent, standardised analytics to our audits. We will also automate the routine data checks needed to undertake audit. This allows financial auditors to focus on data interpretation and deepening their understanding of the clients we audit. Analytics will be designed to analyse 100% of the transactions, in contrast to our current sample-based approach. These analytics will be integrated into our financial audit methodology, and in time will be integrated into our documentation workflow as part of ATP.

32 For previous audit cycles, we have delivered a self-service journals analytic app and a trial balance reconciliation app. In the next 12 months, there are four additional analytics planned, including; self-service journal analytics 3.0, a risk assessment analytic allowing audit teams to explore the general ledger data to identify different audit areas, a PQ query analyser and a reversals app.

> **Digital Plan deliverable (DA03)** – Report on the progress of the digital audit capabilities listed at Annex C

Modernising Value for Money & Investigations

33 Our project to digitally modernise the Value for Money service line will improve the quality and consistency of our outputs through three primary workstreams.

Modernising VFM production

34 **Modernising VFM outputs** – the project focuses on improving the efficiency of the reporting process. Developing a more streamlined solution for managing the publication process, from drafting through to printing. The project team's focus is on modernising the templates used by audit teams and on improving the publication process. The ODP work packages will look at a wider range of VFM and Investigations products to better target the impacts we want to achieve and will explore how technology may assist with their production.

Software, storage & management

35   Audit Software Update/ Data Storage and Management – as with financial audit, the VFM practice is identifying the best technology solution to store and manage VFM audit information. The project will design and pilot an overall solution that will enable teams to collate evidence and link it to their report. The solution will promote compliance and knowledge management whilst managing audit integrity and be scalable and easy to manage. Storage will be standardised as will the production of key outputs. Proposals within the ODP include moving away from MKi to Microsoft Teams and SharePoint and automating the creation of data reconciliations. We aim to exploit Office 365 and Microsoft Teams functionality to increase the efficiency and compliance of standard structures and processes. Digital Services are also coordinating a review on how templates are used and whether there is a better solution for managing formatting and structure in written work.

> **Digital Plan deliverable (DA04)** – The Modernising VFM project will continue to track and publish progress against agreed deliverables

Improvements in Audit Information Management

**36   **Our implementation of an audit information management system (AIMS) supports the NAO's existing client data management needs and provides a platform that will support the long-term goals for managing external data across all parts of the office. AIMS will improve quality, generate insight, and enable the NAO to embed data analytics as standard in all aspects of our audit work. The solution is a scalable, flexible, secure, cloud-based system that supports standardisation of data for the Financial Audit service line and for all client data across the office. The system will be used to manage the flow of all client data into the NAO.

Enhanced data service & analytics

**37   **AIMS will improve the way that we use data across our audits through workstreams to; embed data analytics as business as usual, trial data-led small audits and encourage corporate-wide adoption of a system for managing all client data. It will improve our data analytics capability in the following areas:

- **Making Data Analytics Business as Usual** – To successfully roll out tried and tested innovations in data analytics across the service line which improve both quality and the value of our audit insight. Within this we have a subset of additional projects.

- **Business Process Analytics -** To use data analytics to audit some standard business organisational processes (e.g. purchase to pay; order to cash) to better address audit risk and add value to our clients,

- **Data analytics, client specific pilots** - To discover further opportunities for data analytic approaches that meet specific client needs that could be rolled out across the service line and add value through increased insight;

Simplified approach

38 The service is partially delivered, the infrastructure and supporting security model is in place and is being used by several audit teams. The initial implementation built 'fixed data pipelines' on a client by client basis, this attracts a high level of complexity and relies on teams having a high degree of understanding of the automation requirements upfront. Going forward we are looking to simplify the approach with a small suite of generic upload tools where a central team can assist with the transformation of client data into a format which AIMS can process.

AIMS 1.0 phase 2

39 The delivery plan is for all Financial Audit teams to use the service to ingest their client data into AIMS and use the relevant analytics as part of their audit in 2021. The AIMS team are pursuing four workstreams within a package of work (entitled AIMS 1.0 phase 2) to improve the BAU state for the AIMS service, these are:

(i)   Techniques for getting better data from clients,

(ii)   Making it easier to get data into the AIMS service,

(iii)   Future functionality to design and improve bespoke analytics work,

(iv)   Key enablers of the service, including training, usability and security enhancements, and improving adoption.

40 Analysis and Digital Services teams will continue to collaborate to ensure that the solution manages the transfer, storage and use of all data used to support all audits (including VFM). By the end of 2021, this platform will also host the Data Service and potentially internal business intelligence data.

> **Digital Plan deliverable (DA05)** – Complete roll-out of the AIMS service to all financial audits and delivery of the AIMS 1.0 phase 2 package of work. Review and deliver AIMS 2.0 in 2021

Digital Workplace

41   Our vision of a well-integrated digital environment relies upon digital workplace initiatives which support our people in their daily work as they create and consume content, collaborate and communicate. Recently completed NAO digital projects have seen highly successful transitions to cloud computing, the next two years will see all remaining digital workloads move to cloud. We will complete these migrations while evolving our digital operations to better administer, manage and maintain cloud service provision. At the same time, we will apply continual improvement to the new cloud services to ensure that we continue to maximise the value return from our investments.

42   We have structured our digital workplace initiatives across three workstreams, all of them reflect a highly changed working environment comprising extensive remote and home working. These are:

- **Content, collaboration & continuous improvement** – improving the way we store, access, share and consume NAO information, how we communicate digitally, and how we will continuously improve digital service delivery.

- **Technology enhancements** – completing the transitioning of our digital estate in to cloud service provision, enhancing our extended remote working model, assessing the digital contribution towards the NAO's net zero carbon emissions targets.

- **Information security** – The latest Information Security Plan (2020-2022) builds on our vision to better understand, identify, and manage the threats and risks that impact the NAO's ability to deliver its vision and strategy*.*

43   Our strategic intent for all NAO technology capabilities is outlined at [Annex D](#).

Content, collaboration & continuous improvement

44   This element of the digital workplace workstream covers our plans for enhancing corporate content stores and applications, collaboration capabilities and the continuous improvement of digital service provision.

Content platforms

45   A number of new cloud information stores have been delivered in recent years, including document management & electronic communication systems (Office 365) and a cloud-based Enterprise Resource Planning (ERP) system for managing our people, financial and project resources (Financial Force). These systems are subject to cyclical updates throughout the year and from time to time we review service suitability. For the remainder of the timespan of this Plan we will focus on various enhancements to our ERP platform.

46   A number of these changes have come about because of the NAO's new strategy and the subsequent move to corporate groups and knowledge hubs. We have had to restructure a lot of the data models and hierarchies within corporate systems to reflect this change and as the ERP system is our primary hub which feeds other systems (eg. email distribution lists, corporate

balanced scorecards, and the data warehouse) we have taken the opportunity to optimise data models and update mechanisms. Specific areas that will be enhanced within the ERP system include:

- Changes to our performance management system,

- Enhancements to include new personal development plans,

- A new learning experience platform,

- Ability to access expenses and timecards via mobile devices,

- Functional enhancements for HR, Finance, and central reporting teams.

47 There will also be several enhancements made to corporate reporting data platforms to reflect the new KPIs and balanced scorecards for areas. We will continue to review our corporate dashboards and implement a range of enhancements to support new corporate reporting arrangements under the new strategy.

Digital Plan deliverable (DW01) – Various content platform changes will be tracked and reported at quarterly Service Management Group meetings chaired by Director, Digital Services

Collaboration & conferencing

48 The final stages of this Digital Plan will see enhanced collaboration and conferencing capabilities. We have delivered Microsoft Teams as the next generation tool for managing team content and for our video conferencing services. The next stages will be to;

- determine adoption rates and future ways of working using Microsoft Teams,

- a strategic solution for conferencing and broadcasting services,

- Enhanced Intranet & search capabilities,

- establish external collaboration channels using SharePoint online.

49 Microsoft Teams – Following the successful deployment of Microsoft Teams in 2020 we will deliver a project to review usage, check for consistent implementation and usage at team level, ensure that we are getting the most value we can from the application and that our use reflects good practice. In 2019 we successfully migrated all telephony to Microsoft's Skype service, the next step is to complete a migration away from Skype and on to Teams for all NAO telephony and messaging services.

50 Conferencing – During 2021 we will introduce a strategic video & audio conferencing solution which will see the same technologies applied in every meeting room as are used in one to one video and audio calling from laptops. The solution will follow the architecture principles within this strategy (simple, secure, user-centric and providing long-term integrated value). At this stage we expect the solution to be Microsoft Surface Hub 2s which closely integrate with Skype for Business and Microsoft Teams. Later in 2020 we will review the likely quantities of NAO people who will be at NAO offices and get a better idea of meeting room demand and therefore what our strategic solution for video conferencing will comprise in terms of quantity.

51   Enhanced Intranet & enterprise search – We will complete the migration of all Intranet content and services on to the SharePoint platform which will bring improvements in usability, access to corporate information and better knowledge sharing. Corporate searching will continue to be improved, ways of finding and surfacing content relevant to work being undertaken will also be explored and mechanisms for automating various stages of document management and of the full document lifecycle will be investigated.

52   External collaboration –SharePoint online allows teams to multi-author all office productivity documents (Word, Excel, PowerPoint etc.), this has led to faster turn-around times for creating, editing and reviewing our documents. The next stage in collaborating is to allow individuals from outside the organisation to contribute to documents and indeed for NAO people to contribute to content authored externally. We will look to design and implement this capability in 2021 and then further review how and where it might be used. This clearly has references to the above Modernising VFM project on workflow and reports – there will be several cross-referenced initiatives which will need to be closely sequenced and intent-aligned.

**53   The NAO has a new knowledge management function, going forward the Digital Services and Knowledge teams will work closely together to develop SharePoint for knowledge purposes, this will help shape the composition and sequencing of collaboration and portal capabilities. There are several situations where external collaborations will be beneficial, these include:

- Clearance – where we want our clients to directly input into documents which never leave the NAO network perimeter

- Information and data sharing – portals for external contributors (clients or expert advisers etc.) to securely share data, information or content directly into NAO content or data repositories (particularly linked to AIMS) and a direct replacement for the current 'Huddle' service

- Publishing – where we wish to publish content which others may continue to be able to contribute to post-publication or in an on-going state

- Joint-working – where we use framework partners to perform audits on our behalf

- Extranet services – for example with our local government responsibilities where we can develop secure 'private' external communication channels with partners or with clients

- Parliamentary sessions – we may wish to publish supporting documentation for parliamentary sessions for members or

- Conferencing – Video or audio conferencing with trusted partners or clients involving content sharing

- Secure portals – We may wish to set up secure two-way content portals for specific instances, such as information sharing with our tenants or with other State Audit Offices

- Enhancing external facing communications – introducing capabilities which will promote us as a key repository for public change

  Digital Plan deliverable (DW02) – Various collaboration changes are tracked and managed as part of a Teams project, other activities listed here will be tracked and reported as part of BAU to Executive Director, Strategy & Resources.

Continuous improvement

54   The primary objective for NAO Digital Services (DS) is to maintain, sustain and secure the NAO's digital estate, there are several initiatives scheduled during the lifetime of this plan to improve DS operational effectiveness. These include:

- Setting up a project management office operation to better manage the Digital Services work portfolio,

- Re-tendering our outsourced service desk & digital support service

- Implementing a revised joiners and leavers service

- Reviewing how we deploy software and system upgrades and how groups and objects are managed across the digital estate

55   PMO function – We will implement a PMO function within Digital Services to improve the overall management of the DS work portfolio. This will involve new processes for logging, triaging, tracking, and delivering all digital work packages.

56   Outsourced support provision – Our 5-year partnership contract with Littlefish to provide service desk and broader IT support services to the NAO expires in 2021. We will look to redefine the digital services provided and the associated support service expected from our support provider. A tender exercise will be launched in early 2021 with a view to transitioning to a new partner provider contract in November 2021.

57   Joiners and leavers – We will implement a revised digital joining process for all new staff in the NAO. This will involve reviewing how current arrangements operate and how effective the integrations with other corporate teams are for new entrants and for leavers. The current extended remote working arrangements have highlighted the importance of having an online portal in place for digital equipment provision and the importance of courier services to recover equipment when people leave the NAO. This will be consolidated into a new streamlined service which can be tracked and reported on for effectiveness.

58   Upgrades, security patching & estate administration – Following the successful migration on to Office 365 and Azure platforms we have a range of new technologies available to improve our administration and management of the digital estate. We will review and optimise all our policies, objects and processes for managing all the entities within our network.

> **Digital Plan deliverable (DW03)** – Various Digital Services continuous improvement activities to be tracked and reported as part of BAU updates to Executive Director, Strategy & Resources

Technology enhancements

Cloud migrations

59   Our 5-year program to migrate all digital services and systems in to cloud provision by end 2021 is progressing well and has put us in an excellent position to deal with the challenging scenario presented by COVID-19. Our guiding principle to simplify and optimise services as part of any cloud migration, has ensured that our digital architecture is fully optimised for cloud computing and that we only migrate what we need going forward. We have developed a secure,

repeatable model for cloud migrations and a revised network architecture which will be optimal once all services are migrated.

60   Our approach to utilise software as a service (SaaS) wherever possible has been very successful to date. Some of the remaining services to be migrated will be utilising scripted Infrastructure as a service (IaaS) where the cloud infrastructure is created and managed through programmable scripts. This enables a consistent and repeatable process, which originated from the successful implementation of the AIMS service which will be used as a template for future cloud installations. The remaining cloud migrations include:

- MKi migration to cloud,

- Data Service, Business Intelligence and any remaining on-prem databases,

- DS admin services – backup, system and service monitoring, asset management,

61   **MKi migration to cloud** – This is the last major digital service still operating on non-cloud servers. The cloud migration approach will see all the minor supporting services (monitoring, backup, network management) migrated to cloud once this final system has been migrated. This will enable more dynamic allocation of computing and storage resources as the service requires it and therefore positions us to better manage peaks in the year. This service will complete migration to cloud during the lifetime of this plan.

62   **Remaining corporate databases** – The MKi database is the last significant data store to migrate to cloud. Again once that has completed we can migrate remaining smaller services (VFM Data Service, Business Intelligence and Corporate Reporting). We also have a large legacy data store from our previous ERP solution residing on legacy on-premises servers. We will migrate this (alongside archive MKi data) in to secure cloud storage by 2021.

63   **DS administration services** – Minor administrative services (backup, monitoring, system health & alerts, software deployment, laptop configuration, network management, data integration services etc.) will follow the last major service (MKi) to migrate. These remaining services will take up to 8 months to complete migration and decommissioning. To achieve our end 2021 target for all cloud migrations (and to avoid having to purchase costly hardware to keep systems going) we will need to start minor service migrations before the end of 2020.

> **Digital Plan deliverable (DW04)** – Complete migration of the NAO's digital estate to cloud to be tracked and reported as part of BAU updates to Executive Director, Strategy & Resources.

Remote working enhancements

64   COVID-19 has impacted how and what digital services organisations provide for their people. The NAO has always had a highly mobile workforce and so our digital services and associated development plans have always had enhanced remote working as a key theme. For the remaining timeline of this Plan we have several enhancements that we will introduce which reflect lessons learned from recent events. These include:

- A new remote connectivity model,

- Various security enhancements to better protect our people during extended remote working,

- Increased capacity levels for remote connection networks

- Modern management of digital devices

- A refresh of end user devices (laptops and mobile phones)

65   New remote connectivity – The final element of the NAO's transition to cloud will be to introduce connectivity architectures which negate the need to have network operations within the NAO. The delivery of this new capability will take two forms – a different staff remote access connectivity method and revised systems integration. At present both of these capabilities require an on-premises internal network for staff to connect remotely to NAO systems and for the systems themselves to share authentication information and for data to flow between them. Our new model will enable NAO laptops to connect directly with the cloud services they consume (Office 365, Financial Force etc.) without any need for an intermediary network managed from our London office. Similarly our systems integrate with each other via our network, this new model will enable NAO services on Office 365 to communicate directly with all other cloud services. This will be implemented later in 2020.

66   Various security enhancements – Extended remote working brings a new set of challenges and security risks (see the information security of this Plan). We have monitored NAO staff behaviours and internal & external threats during this period and have a programme of security enhancements which we will implement over the next 12 months. These include;

- New cloud based content filtering services to protect NAO people from accessing malicious or inappropriate Internet sites and services,

- A new unified endpoint security platform (Microsoft Defender Advanced Threat Protection) designed to help prevent, detect, investigate and respond to ever increasing digital threats,

- Multi-factor authentication which utilises biometrics and other mechanisms for staff to securely authenticate themselves on NAO laptops,

- Enhanced monitoring and alerting of events to improve visibility of vulnerable exploits or of suspicious behaviour on our systems.

67   Increased remote capacity – As anticipated we have seen significant growth in remote access bandwidth consumption across our networks, this includes NAO data lines and mobile carrier (O2) networks where staff use the SIM cards in their laptops if home broadband speeds are inadequate. We have steadily increased the capacity from our existing providers, and this has dealt with demand. Going forward we will look to implement a more agile, dynamic and cost-effective solution to better manage NAO needs.

68   Modern management of digital devices – Microsoft have recently launched a new service to set up and pre-configure new devices to ensure they are immediately ready for productive use (Microsoft Autopilot). This service will also be used to reset, repurpose, and recover laptops and phones that are issued to staff (particularly in remote situations). It is a cloud service which simplifies all parts of the lifecycle of Windows devices from initial deployment to end of life and will reduce administration time for Digital Services staff and device downtime for all NAO people.

69   Device refresh – Over the next two years we will also look to refresh the NAO's laptop and mobile phone estate. We will ensure that new laptops and mobile phones provided will be

optimised for remote usage – higher quality cameras, audio and microphones as well as utilising the latest wireless and remote connectivity protocols.

Digital Plan deliverable (DW05) – Enhanced remote working activities to be tracked and reported as part of BAU updates to Executive Director, Strategy and Resources

Net zero, carbon neutral targets

70 **Net zero** – This is an emerging area and so a more detailed outline, plan and specific deliverables will be included in the 2021 update of this plan. The ODP has committed the NAO to achieving net zero emissions by 2029. The steps to achieving this will be included within a detailed environmental action plan which will be launched later in 2020. Across the digital estate there are a range of measures already underway to minimise energy consumption, including;

- Energy efficient digital equipment

- Use of net zero suppliers, logistics and manufactured digital equipment

- Greater use of cloud services and increased remote working

- New digital operating models for all areas of the NAO which eliminate the need for physical outputs

- Increased use of BYOD to reduce the need for NAO supplied equipment

- Use of electronic rather than physical communications and collaborations

- Electronic invoicing and payments

- Externally integrated commerce systems

Digital Plan deliverable (DW06) – Publish digital elements of the NAO's environmental action plan later in 2020

Information Security

71 This element of the plan will ensure that we continue to provide timely and robust assurance on the security and integrity of NAO digital assets. Cloud services provide us with far greater security capabilities than is possible through on-premises computing alone. The assurance capabilities which we get from Office 365, Azure Active Directory and from various software as a service installations (e.g. Financial Force) have been assessed by our internal Infosec team and by external experts and are robust and comprehensive. Cloud services bring greater sophistication and functionality and add complexity, particularly to risk management and the responses required against ever increasing threat. Our strategic approach to how we assess cloud providers and services is outlined in the NAO's Information Security Plan (scheduled to go before the NAO Board in October), within this Digital Plan we focus on three areas where we will further enhance digital assurance across the digital estate over the next three years:

- **ISO27001 & continuous assurance** – Delivering continuous improvement and information assurance

- **Identify, protect & detect** – These dimensions of the Information Security Plan focus on the identification, protection, and detection of threats to the NAO's digital estate.

- **Respond & recover** – These dimensions of the Information Security Plan focus on the response and recovery should threats materialise and the steps to continuously monitor for threats to the NAO's digital estate.

ISO27001 & continuous assurance

72   Earlier this year we achieved ISO27001:2013 accreditation. This is a tremendous achievement and provides an annual process for us to measure our ongoing assurance levels. The specific control areas assessed are; policies, organisation, asset management, cryptography, physical and environmental security, operations & communications security, incident & continuity management, systems development, supplier relationships and overall internal & external compliance.

73   Continuous assurance refers to how we will ensure that there is continuous improvement of the NAO's information security management systems to ensure resilience to withstand and recover from threats and risks which may impact the NAO. Plans in this area span internal and external auditing of processes (IT health checks, penetration checks, privacy impact assessments of systems and services) blended with external accreditation such as ISO27001, Cyber Essentials Plus.

Identify, protect & detect

74   The **IDENTIFY** dimension of the plan focuses on developing an organisational understanding to managing security risk to systems, people assets, data, and capabilities. The key capability areas being; asset management, governance and risk management.

75   **Asset management** – We will improve consistency of digital asset management tools and systems. Similarly patch and functional upgrades to systems will be subject to a review of policy and processes. Digital Services will work in conjunction with Information Security team to improve the agility and maturity of asset management practices. Exploring the use of dynamic asset discovery tools that automatically update databases.

76   **Governance** – We will review how we monitor, evaluate, and direct the delivery and continuous improvement of the information security management system. Having achieved ISO27001 we will operationalise all digital aspects within operating models for all functional areas of the Corporate Group. Within Digital Services this spans change management, design authority and PMO functions. We will integrate security and privacy in to audits and projects to ensure that information security forms the bedrock of all activities containing personal or client information.

77   **Risk management** – We will look to optimise risk management through provide greater clarity to information asset owners and all risk owners of their portfolio of responsibility. This includes exploring options for digitising risk assessments and DPIAs, using data-led quantitative risk management practices to provide greater clarity to the SIRO and to improve the maturity of the NAO's risk monitoring capabilities.

78   The **PROTECT** dimension of the plan focuses on defining appropriate safeguards to ensure delivery of critical infrastructure services, supporting the ability to limit or contain the impact of a potential cybersecurity event. The key capability areas addressed include; identity and access control, awareness & training, data security, information protection processes and

procedures, maintenance and protective technology. These span four key areas; cyber awareness & culture, mitigating against data loss, secure remote working, biometrics.

79   Cyber awareness – The human element is a critical factor of cyber resilience. Phishing and other forms of social engineering attacks continue to be a persistent threat that the NAO needs to account for. Over the next two years we will invest in more personalised, contextual security awareness and communications. There will also be collaborative work with L&D to introduce more inclusive, accessible and sustainable security training solutions that relate to the NAO organisation, culture, values and policies; to apply modern tactics such as personalisation, digital micro-learning, periodic assessment and data-driven analytics to improve learning outcomes and measure progress. The Digital Hub will play a key role in this.

80   Mitigating against data loss – The risk of data loss continues to be the primary information security risk for the NAO. We have a lot of data spanning numerous platforms, data exchange with our clients also operates over various channels. This is a key area which will be addressed during the lifecycle of this plan. We will introduce mechanisms for methods for automatically discovering the data assets that we hold. We will also look at key channels of potential data loss and identify appropriate and sustainable solutions to control and mitigate the risks.

81   Secure remote working – The COVID-19 pandemic and enforced social distancing measures has challenged our approach to secure remote working. The NAO's digital estate has held up impressively to the challenges of extended homeworking for all NAO people and we have demonstrated that the NAO can deliver its objectives successfully through remote working. This sustained working model leads to new emerging threats – for example, our event logging and monitoring systems are not optimised for using digital services remotely all of the time. We will define and deliver a remote working solution that delivers long term sustainable and secure remote working.

82   Biometrics – Identity and access control, particularly in scenarios of sustained remote working, pose a significant security risk. We have several controls in place to protect identities and to control access to NAO systems. We will implement enhanced identity authentication through biometrics on all NAO devices by 2021.

83   The **DETECT** dimension of the plan focuses on appropriate activities required to identify the occurrence of a cybersecurity event in a timely manner. The security plan references the need for a shift in mindset from 'build the walls higher' to 'assume breach'. We will therefore make greater use of technology to proactively detect and respond to all potential threat vectors. This requires focus on two key areas – monitoring and threat hunting.

84   Logging and monitoring – We will operate a centralised, cloud-delivered security incident & event management system such as Azure Sentinel. This will give us greater visibility of meaningful data from across NAO systems and cloud services to proactively detect and respond to security related incidents.

85   Proactive threat hunting – Building on the concept of 'assume breach' one of the opportunities we have with the Microsoft cloud is Advanced Threat Hunting. This enables us to leverage real-time threat intelligence to proactively hunt for indicators of compromise across our estate. Once these tools are operational, we will hunt for dormant, emerging, insider and advanced persistent threats across our digital estate as part of standard operational procedures.

Respond & recover

86   The **RESPOND** dimension of the plan focuses on appropriate activities to take regarding a detected cybersecurity incident. This centres on optimising how we respond to incidents.

87   **Optimising incident response** – The key capability areas include; response planning, communications, analysis, mitigation and improvements. As we transition to a new third party support provider during the lifetime of this plan, we will work with them to ensure that the relevant teams agree procedures, tools and targets for optimal incident response. We have a range of tools available; we will consolidate these to simplify and enhance the process.

88   The **RECOVER** dimension of the plan focuses on appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. An effective recover function supports timely recovery to normal operations, reducing the impact from an incident. Two key areas addressed by this are:

89   **Forensics** – Digital forensics is a very niche and specialist skill, but it is essential to performing root cause analysis for major security incidents and breaches that occur. We will put in place a contingency contract with a specialist digital forensics provider to provide an insurance policy should we suffer a major security incident.

90   **Business continuity & disaster recovery** – we currently are in a state of increased remote working and when combined with our strategy of increased cloud service provision we have demonstrated that existing disaster recovery plans, which assume the loss of on-premises needs to be swiftly recovered needs to be challenged. The cloud does provide much increased availability and continuity in the event of disaster, but it does not mean that we have absolute business continuity, it merely provides the vehicle to deliver it. We must still operate a program of testing our recovery capabilities and look to continuously improve how digital business continuity operates.

> **Digital Plan deliverable (DW07)** – Digital Services and Information Security teams to produce a delivery plan for the next two years and report progress to Executive Director, Strategy and Resources

People & Knowledge

91   This is a new pillar of the plan. Following the launch of the new NAO Strategy and the associated Organisational Development Plan two new themes have emerged which have sufficient digital components to merit specific focus within this plan. They are People and Knowledge. These were briefly touched upon in the first iteration of this plan with the expectation of further expansion once more detailed thinking emerged from the NAO Strategy.

People

92   This corporate theme sets out our plan for becoming a more inclusive and diverse workplace that focuses more on our people; their well-being, management and development. The Digital Plan draws out three key work packages with digital components:

- **Development of digital skills and competencies** – defining the expected digital skills and competencies of all NAO people, establishing baselines, and developing an approach to achieve our targets

- **Improving digital learning & development** – tailoring our approach to digital L&D delivery according to needs, timing, and opportunity

- **Improved employee experience** – Improving the work-life balance and well-being for all, implementing a digital diversity & inclusion plan, making excellent line management the norm, and improving the induction process – particularly for trainees

Digital skills and competencies

93   The NAO has done a lot of work to define core competencies expected of auditors within the two service lines, this typically focuses on a range but primarily on accounting and numeracy skills. As digital competency demands grow, the need to articulate our expectations of core and progressive digital competencies increase. Similarly, within Digital Services (DS) while we stipulate expected skills and competencies within given role descriptions, we are yet to produce a matrix structure of expected competencies and capabilities within each level of the hierarchy. This is key to ensuring fairness and consistency and to providing aspirational targets for our people. There is therefore a need to define a digital skills and competency framework for DS people and, in conjunction with the new Digital Hub and L&D, for the wider office.

94   There are numerous frameworks for assessing the digital skills and competencies of employees, government typically uses [SFIA](#) (the global skills and competency framework for a digital world) and the Government Digital Service (GDS) promotes a cut-down version of this for digital roles in government called the Digital, Data and Technology Profession Capability Framework ([DDaT](#)). Good practice avoids inventing a new framework but customises these existing ones to ensure relevance to the NAO.

95   Over the next eighteen months we will therefore look to articulate core competencies for all roles within DS and wider roles across the office broken down by category. Within DS we will:

- Define technical, functional and non-functional competencies required for each role

- Identify whether individual competencies are critical to each role

- Articulate the level and function of each competency at each level of the hierarchy

- Assess competency and skill level of everyone within each role (needs training, basic, advanced, exemplar)

- Identify development mechanisms for achieving the next skill level for each competency

96 Across the NAO we will look to articulate the core digital competencies expected and, within the Digital Hub, will identify and promote specific development pathways for improvement. Our plans here involve a blended approach to learning, 'digital dippings' as minor introductions for those who wish to have an overview and more immersive digital training for those requiring greater detail which may involve online / classroom or British Computing Society endorsed distance learning. We will analyse what our training needs are as an office and use this to understand what skills are needed in the future and what digital channels might be used to deliver them. The intention being to provide our people with opportunities to develop the knowledge and skills to use our technology effectively, efficiently, and safely

Digital Plan deliverable (PK01) – Produce a Digital Services competency matrix and associated development paths for each competency and role

Digital Plan deliverable (PK02) – Publish expected core digital competencies and development pathways within the Digital Hub

Digital learning & development

97 There is a paradigm shift taking place within training as we transition from learning to contextual guidance, this is expected to have a significant impact on people performance. One of the guiding principles is simplicity & agility. The key underlying principles of agile [in the digital sense] is that every step is small, and everything is subject to change. Our corporate L&D strategies reflect our ambition to transition away from training for knowledge towards training for adaptability. It is vital that our people become comfortable with constant change as we see this in all cloud-based software and we will see more of it in our audit methodologies and approaches. A key element of this transition is for our people to not feel that they need to know all there is to know about a digital service or tool (because that is likely to constantly change) but instead to know where to go for contextual guidance at precisely the time it is required.

98 We are seeing innovators in the digital training industry pivot from long-term knowledge transfer to short-term problem solving. There are emerging solutions which can help build and develop training content libraries. NAO L&D and DS teams will work together with potential providers to identify how to locate and distribute learning and guidance optimally either by system, function, capability, or knowledge hub. The ease with which NAO employees can find the content they need, at the time and form they need it, will be crucial.

99 New digital learning systems utilise forms of machine learning and artificial intelligence to proactively sense a user's needs and then deliver the most appropriate content. Being able to find and apply solutions to everyday problems arising in the flow of work – improved search functionality, rewarding sharing and collaboration, use of chatbots / help screens and guidance as well as curated content from across the web.

100 We are seeing more sophisticated cloud services come with these services baked in. We will look to activate these solutions (which for example come with Office 365 and Microsoft Azure) to monitor user behaviour and offer assistance or 'what other users typically do next' suggestions. We will particularly investigate these concepts within the ATP.

101 Over the next twelve months a team from Digital Services and Learning & Development will look to catalogue opportunities for dynamic learning and produce a programme of digital learning work specifically designed to improve digital learning across the NAO. We will create a blended learning curriculum to provide our people with the support they need, in the format they want, at the time they require it to use our technology. Connecting formal training with informal learning, knowledge-sharing and collaboration via 'nudges', gamification and rewards to increase behaviour change at work and collective performance improvement.

> **Digital Plan deliverable (PK03)** – Produce a catalogue of digital learning opportunities together with a resource plan for delivery

Improved employee experience

102 Improving the employee experience spans all aspects of the People theme of the NAO strategy. There are multiple work packages which directly contribute to achieving this, including:

- Improving work-life balance and well-being,

- Implementing a digital diversity & inclusion plan,

- Making excellent line management the norm and

- Improving the induction experience – particularly for trainees.

103 As part of the refresh to our approach to well-being we will ensure that the office has the right tools to improve our planning of work and allocations. We will develop the concept of a personal digital 'passport' for reasonable adjustments to ensure a personalised digital service is provided to those who require it and to improve awareness, training and support in accessibility tools and functionality. This will also ensure that we take in to account the digital element of personal development plans, motivating individuals to take responsibility for their own continuous professional development in a digital context.

104 We are committed to ensuring that we have a diverse and inclusive Digital Services team. We will determine and publish aspirational targets for BAME and female representation at all levels of seniority across digital. We will ensure that we have BAME/female representation within shortlisted groups and panels for all digital recruitment. We will encourage all working within digital to complete unconscious bias training and testing.

105 As part of our commitment to making excellent line management the norm we will support line managers within digital areas to become excellent through individual tailored training, development, and support. As outlined above, we will ensure that resource systems are adapted to better enable this, for example though; a revised appraisal system and personal development plans for all staff.

106 Following the current period of extended homeworking we will investigate how to improve corporate joining and induction processes from a digital perspective. Tailored assessment and personal development plans for new joiners to ensure they meet the standards of digital competence required as well as providing ways to benchmark themselves and develop their

self-awareness. We will explore how best to digitally support our cadre of trainees from digital learning through to the right levels of digital support for examinations

Digital Plan deliverable (PK04) – Update corporate systems to improve allocations, revise appraisal processes and manage personal development plans

Digital Plan deliverable (PK05) – Implement a revised digital induction process and extended homeworking digital asset management processes

Knowledge

107 This corporate theme sets out our plan to improve how we gather and share our knowledge. The digital elements within the plan for knowledge focus on three key areas:

- **New knowledge model** – designing and implementing a new knowledge model, incorporating new knowledge products and ensuring that we maximise the opportunities presented by new cloud services

- **Wider engagement channels** – overhauling our website, more effective engagement through a variety of digital channels, using tools to exploit the NAO alumni network knowledge better

- **Improved use and re-use of our knowledge products** – Developing and improving current processes and templates for knowledge capture and sharing and explore future options for tools

New knowledge model

108 A new knowledge model will lead to new knowledge products to be managed through existing and new tools. We must make it easier for people to capture and re-use corporate knowledge. We have implemented a range of sophisticated knowledge tools within Office 365 which we are yet to fully exploit. We will work to ensure that digital tools fully support an office-wide approach for how we use, create, and project our knowledge as effectively as possible. We will work with knowledge hubs across the office to ensure that the right digital tools and services are available to support the development of our expertise and knowledge.

Digital Plan deliverable (PK06) – The new knowledge model and associated digital tools to be published in 2021

Wider engagement channels

109 We must work to project our knowledge more effectively through multiple channels. Our website is the primary channel that we use to share our work, we will overhaul the website to enhance accessibility and usability. We will make it easier to engage more effectively through wider online channels, including social media, blogging and video content. To ensure that we produce an effective and achievable target state, we will baseline the use and impact of our knowledge products and activities and collect evidence so that we know what works. We will then use this to shape the knowledge model and identify tools and services to maximise impact.

Digital Plan deliverable (PK07) – Overhaul the website and identify areas where we can better exploit a range of digital channels.

Improved use, re-use and impact

110 We will review our existing knowledge, information, and tools, informing and expanding current knowledge sharing activities. From this we will develop and improve current processes to capture knowledge and explore future options for tools that make it easier to do this well. We will produce templates, products and tools which promote our back catalogue and shared knowledge capabilities better. Hubs will develop consistent and effective knowledge portals to help build and expose repositories of knowledge and expertise. We will also provide digital tools to help relaunch the NAO alumni network to support exchange of knowledge across relevant organisations and sectors.

> **Digital Plan deliverable (PK08)** – Identify tools to improve knowledge capture and re-use, help Hubs to be successful and to exploit the knowledge available within the NAO alumni network.

Digital investment model

111 The table below outlines the NAO's investments in digital across a range of functions and corporate areas (including; Digital Services, Infosec, Analysis, FAPQ, VFMPQ and some L&D elements). The NAO's annual investments in digital over the following three years will be:

Cost Group	Includes	2020/21	2022/23
NAO Services & Applications	Cloud, corporate and data related services, contracts and subscriptions	£1,250,000	£1,235,000
Digital Operations & Infrastructure	Contracts and subscriptions supporting all NAO digital services	£1,132,000	£1,241,000
Digital Security	Figures from the Information Security Plan – covers subscriptions & services	£80,000	£120,000
Digital Learning	Online digital training & services	£20,000	£50,000
Audit Tools	Includes current MKi costs (£120k) and estimated ATP BAU costs (£400kpa) plus £50kpa for VFM tools	£170,000	£450,000
Consultancy	Discretionary assistance with capacity & capability shortfalls	£250,000	£200,000
Capital	Hardware, software assets and asset construction – Note: 2022/23 is a scheduled laptop refresh year	£1,000,000	£2,000,000
Digital Services Personnel	Service & Delivery Management, Digital Audit & Data Development, Cloud Service Development, Content & Collaboration Services	£2,040,000	£2,250,000
Total		£5,942,000	£7,546,000

112 The table above reflects the NAO's investment in digital across multiple functional areas. The majority of the spend is managed by Digital Services, some areas (security, audit tools, learning etc.) are managed by the relevant functional team for that specialist area. Points of note:

- The figures for 2020/21 assume a completion of the migration of the digital estate in to cloud by March 2021. Cloud costs are consumption based so the final figure may reduce if migrations are delayed

- Costs in 2020/21 include a temporary spike to cover COVID-19 related expenditure (online portals, increased remote network bandwidth, enhanced remote cyber security),

- A new support service contract will be let in 2021 which is anticipated to provide a broader range of services at an estimated annual increase of £150,000,

- Increases in digital learning are estimates and subject to a broader training needs analysis being carried out in 2020,

- Audit tools assumes a BAU transition in 2022 for the Audit Transformation Programme with full year subscription costs commencing in April 2022 (this will become clearer later in 2020,

- Capital costs for 2022/23 include a provision of £1.7m for a full laptop refresh, Annual capital costs are expected to revert to a steady £1m after 2022/23,

- Digital Services personnel numbers have increased slightly during the lifetime of this Plan to enable the delivery of the ATP. Several roles have been appointed on two-year fixed term contracts. Ongoing annual costs are expected to revert to 2020/21 levels from 2023 onwards.

Risks

113 High level risks to the delivery of the Digital Plan will be managed through standard operational reporting lines. Below we provide a summary of the strategic risks and how we intend to mitigate them:

Digital Plan Risk Matrix		
Risk	**Description**	**NAO Assurance & Mitigation**
Security	New strategy components, architecture or services lead to a compromise over current security model. Ultimately leading to increased risk of information asset compromise	The Information Security Plan sets out initiatives that will provide assurance over the activities in the Digital Plan. Security will be built into the change process with assessments being conducted on all our cloud suppliers.
Resource Capacity	Insufficient financial or human capital investment available to deliver the NAO's digital ambitions	Periodic review and close management of priorities and initiative sequencing by the Change & Engagement team. Escalation to Executive Director, Strategy & Resources when conflicts / shortfalls arise
Resource Skills & Capability	NAO staff lacking in technical skills. Insufficient technical staff to manage cloud and non-cloud systems during transition	Focus NAO people skills and capabilities on those required for the strategic cloud platforms and core toolset. Active management of capabilities and capacity through training and development.
Architectural Compromise	High volume of tactical solutions not meeting architectural requirements compromise longer term strategic intent	Digital Design Authority meeting regularly to monitor and manage the extent of tactical solution implementation
Delivery Timelines	Sequencing and delivery of strategic systems compromised through delivery taking longer than anticipated	Effective delivery management, project governance, progress monitoring and review and prioritising of conflicting priorities
Organisational Impact	Delivery of elements of the digital strategy having a poor functional fit, compromised integration or untimely sequencing having greater than anticipated impact on the frontline	Regular operational governance, Design Authority input and Change & Engagement management to ensure architectural alignment and early outlier escalation
Architectural Fit with Clients	NAO strategic digital solutions become incompatible with NAO client technologies or architecture. Resulting in issues for information exchange with NAO clients	Ensure that the chosen strategic platforms form the closest possible fit with the direction of travel for our clients. Utilise open standards and architectures. Regularly review client digital activities. At times commission external reviews to ensure NAO's digital direction of travel is in line with public and private sector.

Annexes

Annex A – Architecture Principles

Secure

Principle SE1: Information & data are securely managed assets

The NAO recognises its information and its data are assets valuable to various people across the organisation and we seek to leverage these assets and extract value from them. We achieve this by implementing consistent information and data models within our solutions, and ensure people can securely access the information they require. The assets will be consistently defined, appropriately shared and will be protected from unauthorised use and disclosure.

Principle SE2: Compliance

Business change (and underlying solutions) will be compliant and aligned with relevant policies, guidelines, and frameworks. Compliance with NAO policies and guidelines is required, as well as alignment with wider Public Sector advice, wherever this is advantageous. Change will be delivered through the NAO's governance framework providing the transparency, decision making processes, and quality assurance required through an appropriate quality management system (QMS).

Principle SE3: Business continuity

Business continuity is always considered and appropriate service levels are assured when implementing organisation change within the NAO. The NAO must be able to deliver against its parliamentary obligations and business plan without disruption. Relevant 'problem scenarios' and mitigating actions should be considered as part of all change initiatives. Service availability for different categories of services should also be articulated within service catalogues and new services assigned an availability category as appropriate.

Simple & Agile

Principle SA1: Simplification

The NAO always seeks simplification of its operating model to support a more effective and efficient organisation. There is proactive drive towards reducing proliferation and complexity across our business and in the solutions we deliver. Our default position is one of simplification; solutions should strive toward simplicity and only incorporate appropriate levels of complexity where necessary and where this carries business value.

Principle SA2: Avoid under/over engineered change

Change initiatives and supporting solutions will be engineered in proportion to the problem at hand and should also reflect the small scale of the NAO operation. Information (level of detail) provided should reflect the current lifecycle stage of the change initiative and be limited to the level required to make informed decisions on the best way forward. This supports effective time management and resource utilisation, whilst assuring a suitable level of quality in solution designs.

Principle SA3: Reuse (solution breadth)

Reuse of the NAO's existing enterprise architecture (people, process, information & data, and technology) is considered first in the provision of new or changed user services. This supports a simplified business landscape and higher return on investment from existing resources. The breadth of capability offered by new solutions (flexibility), is considered as a key factor in any investment decisions regarding the introduction of new enterprise assets.

Principle SA4: Process optimisation

Where a valid business case exists, the NAO seeks to improve organisational processes and enhance organisational efficiency through a reduction in manual non-value adding process steps. This should be achieved through the effective use of workflow, process controls, and system automation.

User-oriented

Principle UO1: Business value

Change should be articulated in terms of the business value being created. The value (and benefits) should be clearly stated and linked to the business services being impacted (or created) by the change initiative. Success criteria for all initiatives should also be articulated clearly in terms of business value.

Principle UO2: Be service and user oriented

When undertaking any change, we will be guided by the user experiences and focus on those services we require to effectively deliver against our strategy. Our people are at the heart of our change agenda, and our user services are independent of the technology layer which underpins them.

Long-term

Principle LT1: 'Architecture' best practice

The NAO has adopted an Enterprise Architecture approach to change management, using industry best practise and tailored to the needs of a small organisation. Change initiatives are considered across the full Enterprise Architecture spectrum and incorporate the needs of, and

impacts on, (i) People, (ii) Process, (iii) Information & data, and (iv) Technology domains within the NAO. Articulating change in this manner assures an integrated change capability and supports a holistic approach to the design and implementation of solutions and the delivery of long term business value. Overall an 'appropriate' level of architecture is important.

Principle LT2: Strategically focused

Decision making should be centred on strategic benefit for the NAO. Focus should be on maximising benefit to the organisation over the long term, with consideration given to target business operating models. Tactical decision making should take place within a strategic context. Short term compromises should not be made where this has a negative impact on strategic goals. Change initiatives should be undergo strategic prioritisation in consideration of the NAO's strategy and current operating model (including the availability of resources) to ensure we're investing appropriately.

Principle LT3: Open & integrated technology

Effective integration of technology is viewed as a strategic requirement within the Enterprise Architecture rather than part of each individual solution or system. The NAO seeks to implement an 'open architecture' characterised by easy integration and inter-operability of solutions providing joined up user services. This 'open' nature is fundamental to our target operating model, enabling us to leverage a wider range of available technologies to support innovative, cost effective solutions which can be consumed by users in a variety of methods.

Principle LT4: Manage Enterprise Debt Ratio

All change should be classified in terms of its Enterprise Debt Ratio - Strategic vs Tactical vs Remedial. This better equips the NAO to achieve the optimal ratio of strategic, tactical, and remedial work, better enabling the organisation to achieve its goals, whilst balancing short term needs against long term strategic requirements.

- Strategic: Changes that take you directly from where you are to where you want to be, and may, or may not, satisfy a short-term need.

- Tactical: Changes that satisfy a short-term need, but do not take you from where you are to where you want to be in the most effective or efficient way. Often required when alternative, more practical or quicker solutions are required.

- Remedial: Changes that address enterprise debt (discussed above) within the NAO. This remedial change should also be categorised as Strategic or Tactical in nature.

Annex B – Digital Plan 2020-2022

NAO Digital Plan 2020 – 2022 v2
Angus Waugh
Director, Digital Services

Digital Audit
"Supporting higher quality, more insightful and system-wide audit approaches through proven technologies"

Digital Audit – DA1
Modernising Financial Audit
"ensuring our audits evolve through new technologies and are managed through effective digital systems"

- DA 1.1 – Audit Transformation Programme (ATP)
- DA 1.2 – IT Audit Capabilities
- DA 1.3 – Audit Applications & Automation

Digital Audit – DA2
Modernising VFM & Investigations
"improving the way we deliver VFM audit through better use of available technologies"

- DA 2.1 – Modernising VFM production
- DA 2.2 – Software, storage & management

Digital Audit – DA3
Audit Information Management (AIMS)
"providing a platform to improve quality, generate insight and embed data analytics as standard in our audit work"

- DA 3.1 – Enhanced Data Services & Analytics
- DA 3.2 – Simplified approach
- DA 3.3 – AIMS 1.0 phase 2

Digital Workplace
"Supporting NAO people to create & consume content, collaborate and communicate"

Digital Workplace – DW1
Content, Collaboration & Continuous Improvement
"improving the way we store, access, share & consume NAO information and improve continually"

- DW 1.1 – Content delivery
- DW 1.2 – Collaboration & conferencing
- DW 1.3 – Continuous improvement

Digital Workplace – DW2
Technology
"enabling access to NAO information assets; anytime, anywhere, in the way our people require"

- DW 2.1 – Cloud Migrations
- DW 2.2 – Remote working enhancements
- DW 2.3 – Net zero carbon neutral targets

Digital Workplace – DW3
Information Security
"Providing timely and robust assurance on the security and integrity of NAO digital assets"

- DW 3.1 – ISO27001 & continuous assurance
- DW 3.2 – Identify, protect & detect
- DW 3.3 – Respond & recover

People & Knowledge
"Delivering a step change in digital people development and improving how we create and exploit their knowledge"

People – PK1
Developing our people digitally
"Providing systems and support for our people's digital growth"

- PK 1.1 – Development of digital skills & competencies
- PK 1.2 – Improved digital learning
- PK 1.3 – Improved employee experience

Knowledge – PK2
Improving knowledge creation and exploit
"Radically improving the use of our knowledge"

- PK 2.1 – New knowledge model
- PK 2.2 – Wider engagement channels
- PK 2.3 – Improved use, re-use and impact

Annex C - Digital Audit Capabilities & Strategic Intent 2019 – 2022

Capability	Current Tool	Strategic Tool	FA	VfM	Internal	Strategic Intent			
						2019	2020	2021	2022
Analysis Tools	PASW/ATLAS/STATA/QGIS/OAK/@Risk	As current	Yes	Yes	No	Maintain	Maintain	Maintain	Maintain
Application Sharing	Shiny Server / Shinyapps	TBD	Yes	Yes	No	Maintain	Cloud	Maintain	Maintain
Audit Management	MKi	TBD	Yes	Yes → No	No	Trial Cloud	Cloud / Review	Innovate / Re-tender	Grow
Audit Data Management	CatFlap & Data Service	AIMS	Yes	Opportunity	No	Innovate	Grow	Grow	Maintain
Bank Confirmation	Confirmation.com	Confirmation.com	Yes	Partial	No	Maintain	Maintain	Maintain	Maintain
Business Management	FF / XCD / SF	FF / XCD / SF	Yes	Yes	Yes	Maintain	Maintain	Re-tender	Maintain
Collaboration	SharePoint / SfB (O365)	O365 / Teams	Yes	Yes	Yes	Maintain	Grow	Maintain	Maintain
Copy Editing	Style Writer	Style Writer	Partial	Yes	No	Grow	Maintain	Maintain	Maintain
Data Visualisation	Tableau / R	Tableau / R	Yes	Yes	Yes	Maintain	Cloud	Grow	Grow
Data Transfer	Huddle	O365	Yes	Opportunity	Opportunity	Maintain	Innovate	Maintain	Maintain
Data Sampling	IDEA	MUS Toolbar / AIM	Yes	No	No	Innovate	Retire	Maintain	Maintain
High Powered Compute	Stand alone PCs	Azure VMS	Yes	Yes	Yes	Trial Cloud	Cloud	Maintain	Maintain
Knowledge Management	SharePoint & apps	Azure VMS	Yes	Yes	Yes	Trial Cloud	Cloud	Maintain	Maintain
Report Templates	Word Template	TBD	Partial	Yes	Partial	Innovate	Grow	Maintain	Maintain
Statistical analysis	SPSS R Stat	TBD	Yes	Yes	Opportunity	Maintain	Cloud	Maintain	Maintain
Surveys	Survey Monkey	Survey Monkey	No	Yes	Yes	Maintain	Maintain	Maintain	Maintain

Annex D – Technology Capabilities & Strategic Intent 2019 – 2022

Technology Capability	Current Tool	Strategic Tool	Cloud?	Strategic Intent			
				2019	2020	2021	2022
Agile Project Management	Team Foundation Server	Azure DevOps	Yes	Review	Cloud	Maintain	Maintain
Backup	Net Backup	Azure Backup	2020	Innovate	Cloud	Maintain	Maintain
Device Management	SCCM	Intune Autopilot	2020	Review	Cloud	Maintain	Maintain
Digital Telephony	SfB & Cisco Call Manager	Microsoft Teams	2019	Innovate	Cloud	Maintain	Maintain
Document & Records Management	SharePoint online	As current	Yes	Migrate	Maintain	Maintain	Maintain
Follow-me Printing	Canon	Web hosted (GovPrint?)	2021	Maintain	Review	Innovate	Maintain
Incident Management	HEAT	Review in 2020	Yes	Maintain	Review	Innovate	Maintain
Integration Services	Integration Hub	Logic Apps	2020	Review	Cloud	Maintain	Maintain
Perimeter Protection	Fortinet	Firewall as a Service (Az Fw)	2020	Maintain	Cloud	Innovate	Maintain
Remote Access	Direct Access	AOV	2020	Review	Innovate	Maintain	Maintain
Software Management	SNOW	As current	Yes	Innovate	Grow	Maintain	Maintain
System Monitoring	SCOM	Azure Monitor	2020	Review	Cloud	Grow	Maintain
Threat Protection	Windows ATP	Advanced Threat Protection	2020	Review	Cloud	Maintain	Maintain
Video Conferencing	Polycom, Logitec, Hubs, SfB	SRS & Surface Hub 2	2020	Review	Innovate	Grow	Maintain
Vulnerability & Intrusion Detection	Tenable	As current	Yes	Innovate	Grow	Maintain	Maintain

Annex E – Digital Plan 2020 – 2022 Deliverables

Pillar	Theme	Deliverables & RAG rating	Activity summary (July 2020)
Digital Audit	Modernising Financial Audit	• ATP technology implementation (DA01) • ATP technology implementation (DA02) • Digital audit capability update (DA03)	• ATP to articulate where the AMR establishes new ways of working interface with technology • Determine the best technology solution for the NAO, implement for 2022/23 audit cycle • Track and report on the progress of new applications for audit teams
	Modernising VFM Audit	• Modernising VFM production • Software, storage & management (DA04)	• ODP activities to simplify processes and streamline publication • Alternative to MKi will be SharePoint & Teams for VFM teams • Modernising VFM project to track and report on progress
	AIMS	• Enhanced data service & analytics • Simplified approach • AIMS 1.0 phase 2 (DA05)	• AIMS development to be integrated into ATP, AIMS v1.0 phase 2 approved by Head of Service Line • Various technology updates scheduled for 2021/22 as part of AIMS v2.0 and service line expansion • Commenced roll out across the financial audit portfolio, scheduled to complete in 2021
Digital Workplace	Content, Collaboration & Continuous Improvement	• Content delivery (DW01) • Collaboration & conferencing (DW02) • Continuous improvement (DW03)	• Improved FF interface, Groups alignment, balanced scorecard, access through mobile apps • Microsoft Teams, external collaboration portals, • Wider pilot scheduled for summer 2020, full telephony migration to Teams in 2021
	Technology	• Complete cloud migrations (DW04) • Remote working enhancements (DW05) • Net zero carbon neutral targets (DW06)	• Complete cloud migrations by end 2021 • Remote working activities to be tracked & monitored as BAU • New digital emissions targets contributing to corporate net zero target by 2029
	Information Security	• ISO27001 & continuous improvement • Identify, protect & detect • Respond & recover (DW07)	• Successfully achieved ISO27001 ongoing BAU activities to maintain accreditation • Digital Services and Information Security teams to produce a joint plan, progress to be tracked as part of BAU backlogs and reported to Executive Director, Strategy & Resources.
People & Knowledge	People	• Development of skills & competencies (PK01, PK02) • Improved digital learning (PK03) • Improved employee experience (PK04/05)	• Articulate core digital skills and competencies for NAO roles. Conduct a high-level training needs analysis. Publish development pathways for progressing • Catalogue opportunities for dynamic digital learning, produce and commence a delivery plan • Updated systems for appraisals, personal passports & PDPs. Further develop the induction process
	Knowledge	• knowledge management model (PK06) • Wider engagement channels (PK07) • Improve use, re-use and impact (PK08)	• New knowledge products, promote greater use of Hubs, review NAO website • More influential communication approaches, improve understanding of audited bodies • Identify tools to improve knowledge capture and use, re-use existing content, re-launch alumni

Annex F – Digital Plan 2020 – 2022 Technology Roadmap