Home Office

Technology Strategy

Delivering better and cheaper technology

Enabling a data-driven organisation

Changing what we want to change quickly, quickly.

"From a fragmented, tightly coupled, vertically integrated and loosely controlled infrastructure to a disaggregated, loosely coupled and tightly controlled infrastructure"

Contents:

1. Executive Summary

Customers and employees rightly expect modern technology which helps customers receive the service they require and supports employees in protecting the public. We are increasingly reliant on technology to support the Home Office in its role to lead on immigration and passports, drugs policy, crime policy and counter-terrorism, and to ensure visible, responsive and accountable policing in the UK

We need technology which supports the transformation of the Home Office and the modernisation of our processes making them fit for a digital future. We need technology which:

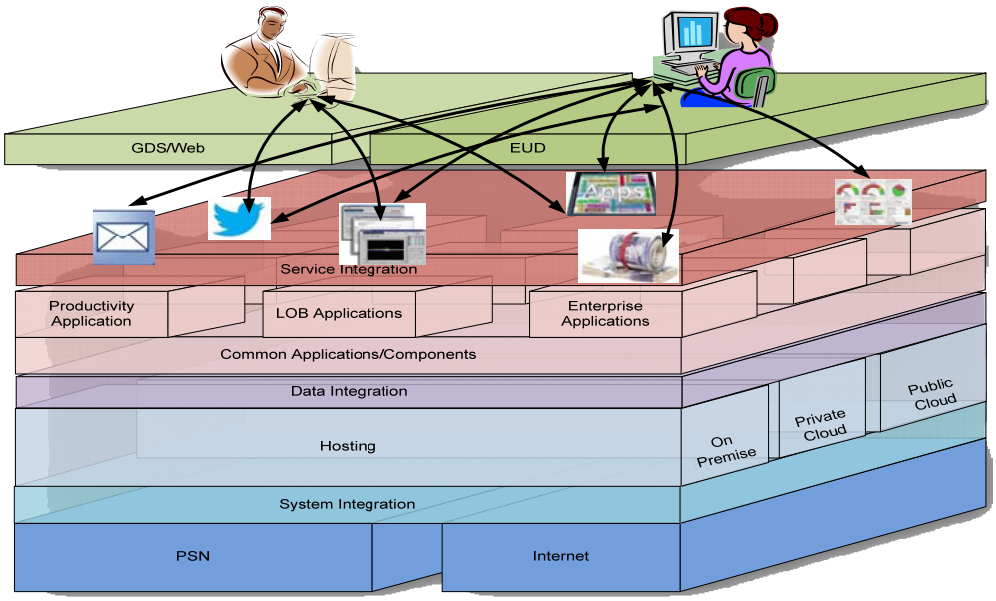
- is better and cheaper;
- enables a data driven organisation;
- allows us to change what we need to change quickly, quickly.

Our current technology does not, and will not, meet this ambition. We need to move:

- from a scarcity of IT professionals to growing capability and capacity;
- from expensive, fragmented and proprietary technology controlled by others to flexible, proportionate and reliable solutions based on open standards and an open architecture controlled by us; and,
- from system design being business area driven to being enterprise driven.

The technology strategy prescribes an architecture for the whole of the Home Office that describes how the Home Office will create a flexible and interoperable approach to delivering future technology and digital services. See annex A for a full description of the enterprise architecture model which is set out below:

Figure 1: The Home Office enterprise architecture:



We will have enterprise control of architecture and separately deliver:

- standard End-User Services bought from standard government frameworks:
- A single Service Integration function with a combination of in-house and outside expertise, which ensures the technology works;
- standard Applications bought in as commodities and mission critical applications which deliver standard business capabilities using common components whenever this makes sense;
- the ability to manage and analyse all Home Office Data as a corporate asset to drive our business activities;
- multiple System Integration suppliers working to a common framework;
- standardised Hosting with a presumption for cloud hosting; and,
- a single Home Office Network built on the Public Services Network (PSN).

The strategy will be delivered through (and constrain) major programmes and the renewal and reshaping of existing contracts. Increasingly we will source our infrastructure from common Government platforms and we will concentrate on delivering our mission critical capabilities:

- enabling interoperability of voice and data for blue light services;
- checking people and goods before they travel and/or at the point of arrival;
- structured application and decision making for status (passports and visas) and background criminal records checks;
- making hard (ie facts) and soft (ie intelligence) information available to law enforcement agencies;
- investigation and case support tools;
- Tier 2 (Secret) knowledge work; and

- lawful intercept of physical and electronic communications.

This strategy is about doing technology differently to help the transformation of the Home Office. Technology is a people business and the strategy talks primarily to those people.

The reform of technology is part of the transformation of the Home Office, complementing a whole suite of activity. Technology is never the whole answer to any question; if it is presented as the whole answer the question is wrong.

2.Introduction

We need a new approach to technology. Customers and employees rightly expect modern technology which supports employees in performing their jobs. This strategy sets out the case for change and the technology response.

Implementing the strategy, through our major programmes and the renewal and reshaping of existing contracts will ensure that we have technology which:

- is better and cheaper;
- enables a data driven organisation;
- allows us to change what we need to change quickly, quickly.

This strategy is consistent with the Government's technology strategy. Our intent is to move from a fragmented, tightly coupled vertically integrated and loosely controlled infrastructure to a disaggregated, loosely coupled and tightly controlled infrastructure.

3.Scope

This strategy applies to the whole Home Office enterprise. That is all functions funded in whole or in part by the Home Office, with the exception of local police technology, the Security Industry Authority (as an independent entity) and the Independent Police Complaints Commission (given its unique statutory position).

4. Our requirement

The Home Office's role is to lead on immigration and passports, drugs policy, crime policy and counter-terrorism and to ensure visible, responsive and accountable policing in the UK. Our users are:

- Customers who expect us to be easy to access, efficient and helpful. We should be able to change our systems quickly in response to feedback and all of our activity should be digital by default;
- Officials who expect us to provide modern tools which help them protect the public, technology which enables them to do the value adding work where judgement and experience are key. Tools which can change and evolve readily as needs change; and
- The body corporate which needs us to provide cheaper technology and enable a data driven organisation.

4.1 Customers / service users

Our major public interactions are transactional and set out at Figure 2:

Figure 2: Major Public Interactions

	Interactions per annum (approx.)
Border Crossing	100m people each way and 180m tonnes of goods
Immigration and Visas	4 m
Passports	6 m
Criminal Records	4 m
Civil registration certificates	2 m

4.2 Our staff

Our staff fall into seven groups, as shown in Figure 3:

Figure 3: Who have we got?

	Number 000s	**Where?**
Knowledge/policy	6	HQ and each delivery arm
Transactions caseworkers	20	Immigration, Passports, Criminal Records
Fixed frontline		Borders (Primary Check Point), Public Enquiry Offices and Passport Offices
Peripatetic/fieldworkers	2	Immigration enforcement and compliance, Borders at non-fixed control. Increasing requirement.
Specialist users - "boffins"	0.5	Scientists, researchers, economists, statisticians

	Number 000s	Where?
Specialist user – "at secret"	4	Serious and Organised Crime Agency(SOCA)/ National Crime Agency, Office for Security and Counter Terrorism (OSCT), limited Borders/Immigration
Critical National Infrastructure enablement for Law Enforcement Agencies	-	Use of applications is generally mediated. Airwave direct provision. Police National Network (PNN) via Frameworks.

All of these staff have standard technology needs and many of them also have particular requirements to fulfil their roles.

4.3 Mission critical capabilities

The Home Office has particular, or mission critical, requirements for both our staff and to provide a national infrastructure for law-enforcement. The mission critical capabilities are:

- enabling interoperability of voice and data for blue light services;
- checking people and goods before they travel and/or at the point of arrival;
- structured application and decision making support for status (passports and visas) and background information criminal records;
- making hard (ie facts) and soft (ie intelligence) information available to law enforcement agencies;
- investigation and case support tools:
- provision of capability for Secret knowledge work; and,
- lawful intercept of physical and electronic communications.

A fuller description of these capabilities is in Figure 4:

Figure 4: Key capabilities – what do we need?

Capability	Current Delivery	User Base	Target Delivery
Enabling interoperability of voice and data for blue light services	Private network (Airwave) and enabling data network (Police National Network - PNN).	Blue light services and other (including covert)	Base on public networks with government role to enable and ensure access and reliability.
Checking people and goods before they travel and/or at the point of arrival to identify targets of known interest and targets of potential interest.	Warnings Index, Semaphore, Freight Targeting, Cyclamen. Warnings Index (WI), Semaphore (S4) and Freight Targeting Systems (FTS) take feeds from a variety of Home Office international and cross government systems.	Circa. 140 locations, 24/7, circa. 100m passenger movements per annum (all checked) and circa. 180 tonnes of non-EU freight (risk based checking).	Separate out application layer, rationalise and componentise based on evolution from current, delivering improved resilience and improved functionality. Scanners and detection devices increasingly networked.

Capability	Current Delivery	User Base	Target Delivery
	Various supporting data and applications used, some supplied by HM Revenue & Customs. Free-standing scanners and detection devices.		
Structured application and decision making support for status (passports and visas) and background information criminal records. Production of status documents (vignettes, passports and Biometric Residence Permits (BRPs). Minority of more complex interactions (e.g. appeals and asylum support).	Patchwork of legacy applications, predominantly in vertically integrated stacks. Operates on UK and Foreign and Commonwealth Office (FCO) infrastructure. Passport (De La Rue) and BRP (Driver and Vehicle Licensing Agency) production centralised.	Public facing application on web and by post. Face to Face in Public Enquiry Offices, Passport Offices, Post Offices and Visa Application Centres. Caseworkers in UK and overseas.	Digital by default for customer interaction. Level 4 identity verification required for passports and visas. Componentised back end systems.
Making available to Law Enforcement Agencies hard (i.e. facts) and soft (i.e. intelligence) information about suspected and actual criminals so the right information is in the right place at the right time. Data is biographic and biometric (facial, finger and DNA (Deoxyribonucleic acid).	Key applications are Police National Computer (PNC), Ident1, National DNA Database (NDNA) and Police National Database (PND). Variety of delivery mechanisms.	Frontline Law Enforcement Officers. Consumption typically mediated by host organisation.	Subject to agreement from Home Secretary, Home Office role to be delivery of data platform and "standards based" intervention in business applications.
Investigation and case support tools: analytics (for intelligence) and case management.	Intelligence and case support capability in a range of applications and commercial constructs.	OSCT, SOCA and Immigration enforcement.	Improved data and analytical capability. Componentised delivery (over time) with increased re-use of core components. Plans not developed for case management.
Provision of capability for the handling of Tier 2 knowledge work and fieldwork.	OSCTnet, SOCA 2010, Mycroft	OSCT, SOCA and Immigration enforcement.	Proposed shared service for knowledge workers. Plans not developed for fieldwork.
Lawful intercept of physical and electronic communications.	Specialist functionality.	OSCT, SOCA and Immigration enforcement.	Specialist functionality.

5.The case for change

The technology we have today and the way it is delivered does not and will not support the transformation and modernisation of the Home Office. We need to move:

- from a scarcity of IT professionals to growing capability and capacity;
- from expensive, fragmented and proprietary technology controlled by others to flexible, proportionate and reliable solutions, based on open standards and an open architecture controlled by us; and,
- from system design being business area driven to being enterprise driven.

5.1 IT Professionals

We need to change how we recruit, retain and develop our IT professionals to ensure we have the right people with the right skills, and that we are able to place them where they are needed across the Home Office. To deliver the transformation outlined in this strategy, and create a data-driven, fully digital Home Office, we need a different range of capabilities to those we currently possess, and we must build this capability quickly. This is recreating the "IT brain" of the Home Office; a brain that was outsourced in the 1990s. We will take advantage of the range of cross government capability initiatives that are already in place, but we must retain a strong internal focus on the development and retention of our IT capability.

The technology industry in the United Kingdom has a range of skill shortages and these are mirrored across government[1] and include business analysts, IT procurement specialists, architects, security specialists and service level management roles. Many of the IT professionals with the skills we require are choosing to work in the private sector. We need to do more to attract the right capability and grow the IT profession, through expanding our apprenticeship and fast stream programmes, providing clear career paths, streamlining the recruitment process and showcasing the benefits of working within government as an IT professional. We need to be more creative at advertising our posts through a more varied range of social and IT networks used by graduates and IT professionals.

Alongside specialist technical and business analyst capability, we need to strengthen our commercial and programme and project management skills (where we also need to develop greater capability in leadership).

5.2 Flexible, proportionate, reliable solutions

The Home Office Digital Strategy outlines our plans to become a digital-by-default department. This will transform the way we manage and publish information, deliver services and develop policy; to achieve this we will need to adopt a new approach to developing, delivering and managing our technology and data.

We need systems that can be improved or adapted quickly, in response to changing business or customer needs. At present, we continue to run a large number of legacy systems to 'sweat our assets' across various business areas, even though newer technologies or more efficient methods are available. These legacy systems are inhibiting change (they usually run on slow or obsolete technologies that can be hard to maintain, improve or expand) and they are more likely to have security vulnerabilities. In addition, integration of legacy systems with newer systems is usually complex and costly. As we move

[1] A snapshot of Government's ICT Profession in 2011 by National Audit Office

from legacy systems and hardware we will see the complexity of technology reduce and business areas will benefit from increased agility and efficiency.

The ways we procure and develop our technology must change to enable faster, cheaper delivery. As large, monolithic contracts expire over the course of the next three years, we will break these up and move to smaller contracts with a wider range of innovative suppliers. As we adopt the Cloud First approach, and converge onto government commodity services where appropriate, we will take control of our IT infrastructure in-house.

Both the Government ICT Strategy and Digital Strategy emphasise the use of technology to provide more cost effective and efficient solutions. Automation is central to this. Where we are still reliant on inefficient, paper based, manual processes (for example for immigration decision-making and border checks) we will automate our processes and systems to support faster transactions, higher quality information and improved customer service.

The ways we work are changing: increasingly business areas need their staff (particularly those working on the front-line) to be able to work in a mobile, flexible way so they can access applications wherever they are, irrespective of location or device, and including at Secret. A fully mobile workforce, with access to all of the systems and information they need, will help to improve the overall effectiveness of our organisation, as well as ensuring we make best use of our property estate and supporting more cross-department working.

We are also moving towards models of more open policy making and service design; policy and services will be developed through a process of active engagement with citizens and business. To support this change, and the commitment to work more transparently, we need to provide appropriate levels of access to social media and other technologies and commit to making information accessible. Our technology needs to enable this, not act as a barrier.

5.3 Enterprise-driven

We need an enterprise approach to information and technology provision to drive down costs and complexity. This includes making best use of common hosting solutions, information architectures, Public Services Network (PSN) and End User Devices (laptops, tablets etc) as well as adoption of the Cloud First approach.

We have failed to reuse assets and ended up with siloed applications because we have not had a strong technical design authority, because we have thought about ourselves in silos, because we have thought about applications rather than business capabilities and because we have concentrated on the differences rather than the similarities within our organisation. This has resulted in expensive and inflexible technology which does not meet corporate needs.

With the ability to effectively (and securely) share information and collaborate across boundaries becoming increasingly essential to all of our business areas, we need to treat data as a key corporate asset - timely, efficient and secure information sharing is critical for the effective business of government and the delivery of public services. We produce and analyse a vast amount of operational and other information, including that relating to visas, passports and criminal records – but as much of our information is stored in particular, business-specific operational systems, we have limited ability to share information. The lack of an overarching technical and information framework has now become a barrier to mapping out the key interactions and information flows required within and across business areas for future improvements, including sharing information across the public sector and with business and citizens. Our technology must enable the smooth and safe flow of data across our own systems, and

more widely, to support better decision making and provide intelligence that will add value across our organisation and services.

This lack of an overarching technical and information framework also extends to digital channels where customer journeys are fragmented and inconsistent and often underpinned by manual paper based processes.

Appropriate management of our information assets, systems and processes is an important aspect of our technology arrangements. The Knowledge and Information Management (KIM) profession in the Home Office have helped develop and put in place a strong set of policies, systems, process and a robust set of security measures. Given the increased focus on the internet for delivery of services, we need to ensure that we continue to keep our information and data safe and secure whilst balancing this with transparency, openness and improved service delivery.

The current review of the Government Security Classification policy provides an opportunity to introduce a much simpler and more intuitive security classification marking scheme. This should allow us to drastically reduce the number of decisions that are required before determining the security marking of a document or sending an email. This in turn will lead to more consistency and will allow us to use more commoditised technologies that cost less.

5.4 We need to:

Taking this diagnosis, we need a technology strategy which helps us to:

- Continue to steadily increase the performance and reliability of our systems whilst, on a like for like basis, reducing cost.
- Accept that there is a commonality of activity (across the Home Office) and, therefore, business areas really can move away from their 'siloed' technology provision to corporate technology capabilities.
- Accept 'good enough' solutions (80/20 rule) to deliver business benefits, avoiding the added complexities and cost which invariably come from more tailored technology solutions.
- Work closely with Cabinet Office and other government departments to ensure central initiatives, on which we are dependent, are delivered on time and as defined.
- Regard our technology enterprise as one organisation rather than separate business silos, plan and resource technology work corporately and have a funded plan for the whole organisation rather than for individual business areas.
- Accept more risk but manage it better in order to take advantage of better value technology approaches.
- Ensure that change initiatives (programmes and projects) agree a common approach to technology solutions in order to deliver quickly and reduce costs.
- Ensure the technology and business communities are partners in the early engagement process when developing policy, strategy, business plans and change initiatives.
- Change and develop our technology and Knowledge and Information Management (KIM) professions so that we have the capacity, capability and flexibility across the organisation to move from assuring suppliers to ensuring service.

- Require business areas to consider process and procedural changes before seeking technology solutions - technology is not always the best answer.

5.5 Benefits:

The implementation of the strategy will deliver - and be judged against - the benefits of cheaper and better technology, enabling a data-led organisation and allowing us to change the things we need to change quickly, quickly.

Cheaper technology:

- We will reduce costs through greater levels of re-use of existing assets, and increasingly use government wide Shared Services.
- We will move away from current expensive monolithic contracts with their potential future commercial and technology lock-ins by breaking up existing services.
- We will benefit from usage based pricing and fast procurement by defaulting to cloud-based solutions (called Cloud First).
- We will drive down the cost of our devices (laptops, tablets) and related services (video conference, contact centres) by purchasing them as commodities, just like we consume electricity or rent premises.
- We will reduce costly and often confusing duplication, by creating increasingly unified and uniform data stores.

Better technology:

- We will provide better, joined up services to citizens, business and overseas visitors by creating end to end digital processes.
- We will provide greater re-use opportunities for our systems by designing them around end to end delivery and not around organisational or process boundaries.
- We will build technology services with the flexibility to be able to respond quickly to changes in policy and business rules and that can be introduced quickly and more cost effectively.
- We will provide better collaboration tools and supply the appropriate technology tools and support so staff can perform their roles in an increasingly mobile and flexible environment with differing profiles of mobile working (i.e. office, home, always remote, etc).
- We will have better control over our technology by assuming more responsibility for delivery of technology within our organisation, particularly around systems and service integration as an increasing number of our services will be delivered by a variety of suppliers of different types and sizes.

Be more data-led:

- We will be able to exploit large and complex information sets to provide better levels of intelligence and customer service by creating more suitable and accessible data stores.
- We will be able to access and share appropriate information more easily at the correct level(s), with trusted partners by putting in place a common data platform across a matrix of protective levels to enable appropriate and secure access to systems and information.
- We will provide more reliable and relevant management information and metrics around process and system performance so we can make comparisons more easily and become more open and transparent about our performance across the organisation.

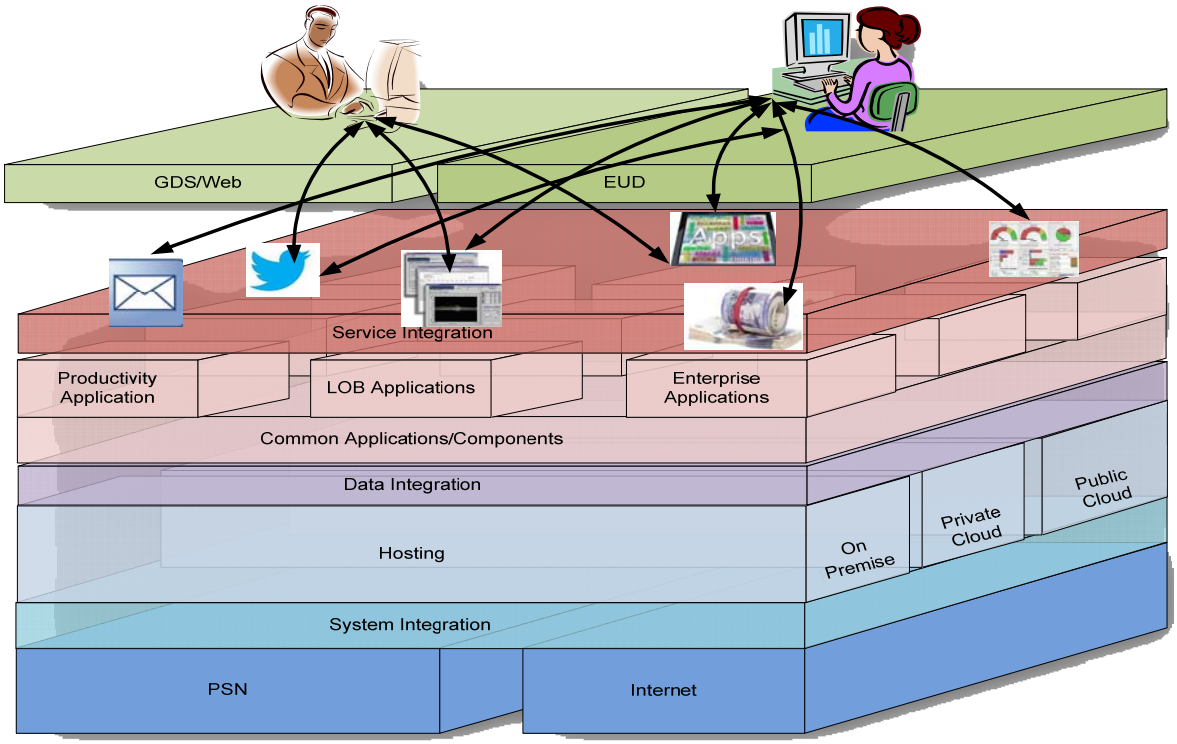
Do things more quickly:

- We will introduce greater speed and flexibility to technology enabled business change.
- We will be more responsive to changes in requirements by delivering our technology iteratively and by using common components.
- We will help enable the business to take greater configuration control.
- We will significantly reduce the effort for projects and programmes to create local technology solutions and help accelerate the pace at which change can be delivered by adopting a common set of architectural tools and standards across our organisation.

6.The technology prescription

The Home Office has not had a directive technology strategy. The case for change has been made and we need to move from a fragmented, tightly coupled, vertically integrated and loosely controlled infrastructure to a disaggregated, loosely coupled and tightly controlled infrastructure.

The enterprise architecture for the whole of the Home Office is defined in the diagram below. A full explanation of the Home Office architecture can be found in annex A:



We will have enterprise control of architecture and separately deliver:

- standard End-User Devices bought from standard government frameworks:
- a single Service Integration function with a combination in-house and outside expertise, which ensures the technology works;
- standard Applications bought in as commodities and mission critical applications which deliver standard business capabilities using common components whenever this makes sense;
- the ability to manage and analyse all Home Office Data as a corporate asset to drive our business activities;
- multiple System Integration suppliers working to a common framework;
- standardised Hosting with a presumption for cloud hosting; and,
- a single Home Office Network built on the Public Services Network (PSN).

6.1 Enterprise control of architecture

The central Home Office Design Authority hub will drive compliance and alignment with Government and Home Office Technology and Digital Strategies and local spokes will provide architectural services throughout the business. This is not just a governance process but a way of working, driving collaboration and corporacy.

To enable consistency across the organisation and to support enterprise wide planning, we will develop a series of products (design patterns, standards, models and principles) and business services (solutions architectures) that deliver against the needs of our organisation at project and business level, and are industry good-practice. This will ensure that:

- we have an open architecture based on open standards;
- technology enabled business change (primarily delivered through programmes and projects) is able to propose and deliver solutions which work for the Home Office business as a whole;
- we are best positioned to re-use assets where cost effective and strategically aligned;
- our technology functions are able to rapidly respond and enable changes to the business operation quickly through the flexible use of technology, supported by more agile commercial approaches; and,
- technology fully supports both the consumers of our public services and our business users who depend heavily on ICT to provide those services effectively.

6.2 End user devices

We will use the government wide End User Device agreements to replace current contracts, either at suitable break points or at end of contracts, to take advantage of better value offerings. We will be device agnostic. Where our End User Devices are genuinely unique, eg e-Gates, we will source them separately as a component.

6.3 Service Integration and testing

Service Integration is ensuring that services run. We will have one Service Integration function which builds on the existing Home Office IT Service Management function. The Service Integration approach will address the impact of separating out IT components such as hosting, applications development, security and desktop support, whilst the contracting of different suppliers is underway.

Component services from multiple suppliers will need to be defined in consistent ways with matching terms and conditions and any necessary variation that will be carefully managed. The Service Integration capability will need to be developed centrally to coordinate and manage suppliers and present a seamless integrated service to customers, ensuring that service delivery is focused on business outcomes. We will maintain control of the entire Service Integration function and employ a combination of in-house and external expertise to ensure that the technology works.

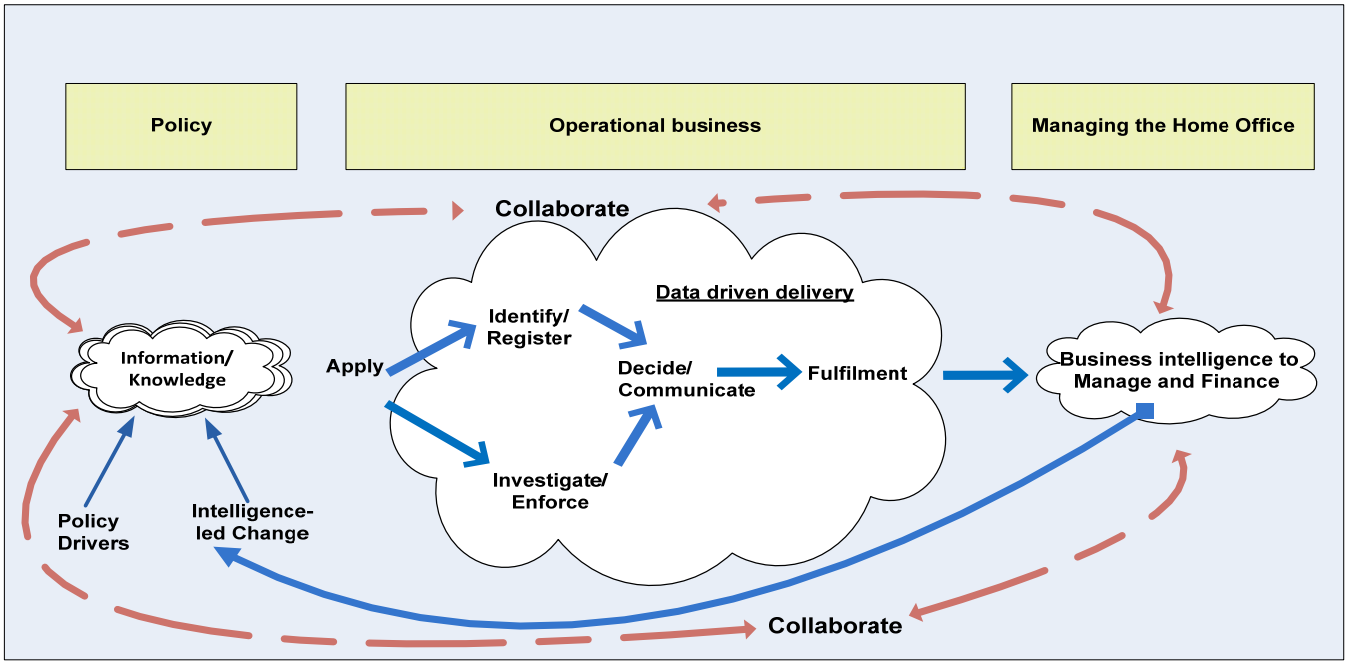
We will continue to develop and improve upon test approaches and structures that best support delivery including agile methodologies, system integration testing, and procurement and delivery through the Cloud. This will ensure we are able to deliver increasingly complex IT solutions that provide high levels of interoperability and integration in a digital environment.

The Home Office IT Test Design and Consultancy Service (TDCS) was set up to improve our test approaches and transform the way IT testing services are delivered across the Home Office Group and wider government. The testing services have been externally accredited to the industry recognised maturity benchmark and individuals within the team are qualified to recognised standards. Risk based testing, using flexible and tailored services, is intrinsic to the TDCS operation.

6.4 Applications

We will purchase standard applications, such as desktop applications and Enterprise Resource Planning tools, as commodities. Our mission critical applications deliver business capabilities which are common across the Home Office. This is because our high level process is common. Figure 5 illustrates how the Home Office applies a common set of high level business processes to deliver end to end services to the public.

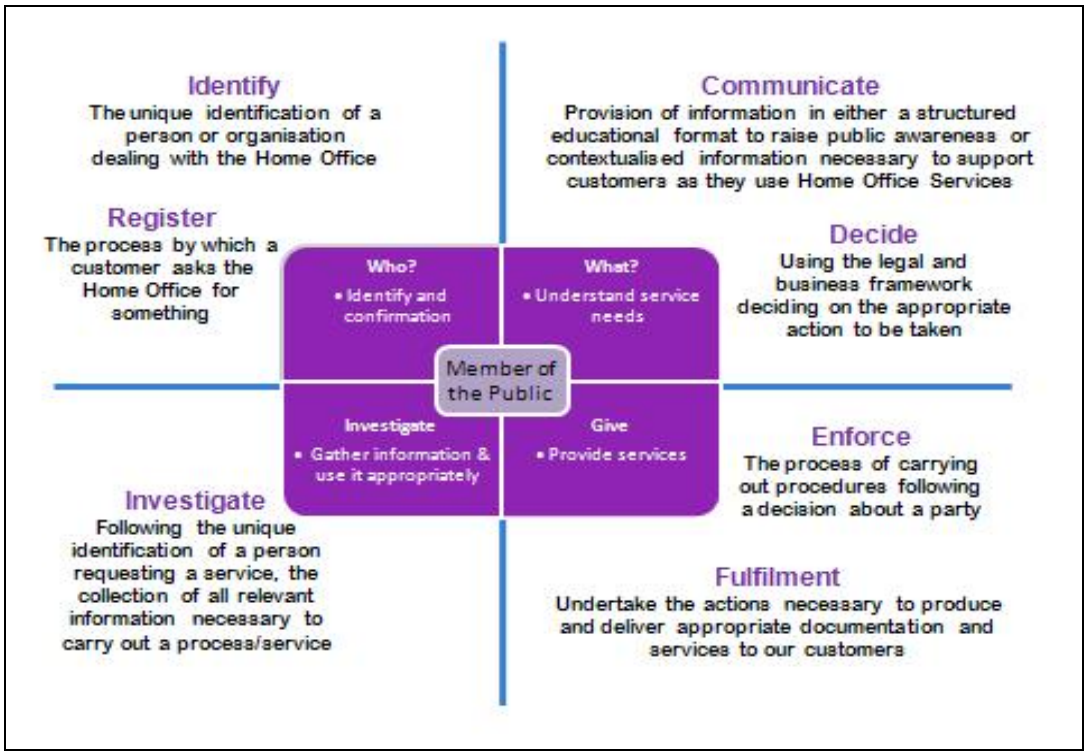
Figure 5: Home Office Generic Service Provision



The 7 high level common business capabilities (Identify, Register, Investigate, Communicate, Decide, Enforce and Fulfilment) that describe how the Home Office operates are set out in Figure 6.

Separating the consideration of business capabilities from IT capabilities will enable us to move away from building big, highly specialised monolithic applications that restrict flexibility and provide a barrier to re-use. Instead, we will use components and applications that are focused on business functionality and can more easily be shared across our various business areas. We will use cross-government platforms, such as identity assurance, where they exist. We will seek to buy and deliver componentised technologies and tightly control the number of bespoke solutions deployed across the organisation. This approach requires commitment from all business areas to use common, sharable components, adapting business processes where necessary.

Figure 6: Home Office Common Business Capabilities



Increasingly we will be able to buy applications from the Cloud. We will adopt a Cloud First approach. This will provide the following benefits:

- usage based pricing to reduce cost so we only pay for what we use and have more clarity on total cost of ownership;
- short term contracts allowing us the flexibility and freedom to change service providers more easily and move us away from lengthy, monolithic contracts that limit change and innovation;
- simply purchasing logins to use applications provided (over the internet) as a fully managed service, rather than buying the software or hardware;
- rapid procurements of whole solutions that are already assured for security, performance and service management;
- greater flexibility to respond to surges in demand; and,
- reducing the demand on our current infrastructure by hosting data and applications in the Cloud.

6.5 Data

The sharing of information though the use of common designs and interlinked technologies will reduce the duplication of data and the delivery of technology solution types. Standard tools and platforms will provide the organisation with greater opportunities to implement innovative ways of using information more quickly for less cost. This will also help to improve the value of information and provide a stronger base for analysis and intelligence.

There are sizable opportunities across our organisation to build on and increase information sharing. There is a range of approaches that the organisation could take to joining up data and information across various business areas. The use of large centralised data stores is an attractive approach, but it

increases the security risks and management complexity so we consider a more federated access system using common data standards as the most suitable approach for our organisation.

6.6 Hosting

We will have a Cloud First policy for hosting and build our capacity to procure hosting as a commodity. Our order of preference is:

- public cloud;
- private cloud;
- on premises.

6.7 System Integration

System Integration is ensuring that the design and build of a system works. To do this, we need to strengthen our integration capability both to bring discrete systems together and to ensure capability within systems can be reused. We will need to:

- integrate systems at the data and functional level irrespective of where they are being run from and who is responsible for their development or maintenance;
- specify interfaces for systems based on open data and open Application Programme Interfaces (APIs) to allow easy flow of data between them;
- carefully plan and actively manage system integration; and,
- closely control interfaces to ensure that there are no disconnects which might make it difficult or impossible to upgrade part of the whole eco-system independently.

This will be delivered by multiple systems integration capabilities working to a common framework.

6.8 Networks

We are committed to aligning with a common and commoditised IT infrastructure across Government. Specifically, we will buy networks through the Public Services Network (PSN) frameworks and will, through the Network Strategy take best advantage of opportunities to consolidate and deliver more cost effective network services. We will have one Home Office network built on the PSN.

6.9 Security

The security of our technology is and will continue to be important. We hold information which must be protected from inappropriate use and cyber attack. The emerging new three tier Government Security Classification proposals is an opportunity to rethink our overall approach to IT Security. We will move from the ‘smartie’ model (all the protection at the outer boundary) to the ‘nougat’ model (hardened at strategic/appropriate points - strength in depth). We will develop a simpler security architecture for the Home Office and will ensure that there is a better balancing of operational risk (arising from information not being in the right place at the right time) with IT security risk (data in our systems being used inappropriately by third parties).

6.10 Tier 2 - Security Classification

When the new three tier security classification system is launched, the (vast) majority of Home Office will operate at Tier 1 (Official). However, some functions will operate at Tier 2 (Secret). We are developing a shared service solution for Tier 2 users which will be shared with other departments who have a (minority) Tier 2 requirement.

6.11 Conclusion

This section sets out a clear technology prescription for the Home Office. The prescription applies right across the Home Office. There will be legitimate debate not about the prescription but about the pace at which different parts of the office move to this prescription. The pace will be influenced by current contractual arrangements, capacity, funding and prioritisation.

The strategy is about technology. The reform of technology is part of the transformation of the Home Office, complementing a whole suite of activity. Technology is never the whole answer to any question; if it is presented as the whole answer the question is wrong. Technology enables but does not drive change across the business, and this approach needs to sit firmly with the suite of business change activities.

7. Delivery

Implementing this strategy presents a significant challenge to the Home Office. Its success relies on strong commitment and leadership. Changes are required across the IT community, the business areas and the corporate organisation so that we have a standardised and common information, systems and technology that will enable us to share and use information and intelligence to deliver a better service to the public.

7.1 Opportunities for delivery

In delivering this strategy, we will use a number of key opportunities to accelerate the pace of change within the Department and drive delivery. These include:

- Modernising Immigration Technology (MIT)
- Border Systems Procurement (BSP) and the wider Border Technology Programme (BTP)
- Intelligence Programme
- Electronic Document and Record Management (EDRM)
- Enterprise Resource Planning (ERP) development
- Ending of some of our major contracts from 2014 – 2016

We will work in collaboration with suppliers to introduce as much of the future target model as possible before the current major contracts end. Through the use of more innovative suppliers aligned to more cost effective models we will deliver better outcomes for the business more quickly. This will require a mix of up front funding and funding from savings achieved in moving from existing IT approaches.

7.2 Roadmaps, detailed strategies and implementation plans

The specific and more detailed further plans to deliver the Home Office Technology Strategy will be set out in a series of specific roadmaps which will be developed during 2013.

7.3 Coordination of delivery

We will embrace a collective approach to technology and we need a radical transformation in the way that we buy, deliver and manage IT to better equip our staff and serve the public. We will use standard methods and tools, selected from the best of breed across the Home Office and wider industry.

The IT functions across the organisation will work closely with the information and commercial teams and the technology enabled projects and programmes to ensure that we deliver technology enabled change for the benefit of the organisation as a whole.

We will have better central co-ordination of all elements of technology. We need to agree and map out the most appropriate sequence of activity to meet the organisational demands for technology and we need to set in train clear and consistent portfolio, planning and prioritisation processes to ensure resources and investments are sharply focused on the highest value activities.

8. ANNEX A: Home Office Enterprise Architecture Model

Layer	Definition	How will the Home Office adopt it
GDS (Government Digital Services) / Web	As specified in the Home Office Digital Strategy, the standard delivery mechanism for the public users of services will be the internet. This will be delivered through the common Government platform, GOV.UK, the Government Digital Services (GDS), or through other non-Government web sites.	The Home Office Digital Strategy sets out our aim to redesign all of our transactional services over the next seven years with a focus on user-need. This transformation will begin with three exemplar services: • applications for visit visas (Immigration Enforcement) • the Disclosure and Barring Service - criminal record checks (DBS) • e-Gates at UK borders (Border Force)
EUD (End User Devices)	The concept of a user only interacting with the Home Office services through a PC, whether desktop or laptop, will become increasingly unusable as the services becomes more integral to the work of the user. Increasing use of mobile devices, such as smart phones and tablets, will see the concept of an end user device change, mirroring the consumer market more closely.	Increasing flexibility in the types of End User Devices (EUD) will have to be delivered at reduced cost, more aligned to the commodity prices in the consumer market. The central purchasing power of the Government will be used through the EUD agreements to deliver the cost savings. We will use the EUD agreements to replace current contracts either at the end of the contracts or another suitable break point. A common infrastructure with multiple EUD interface options will be required.
Service Integration	Ensures that the end user has a common view of services when they have different providers and different delivery models. Allows the user to concentrate on the delivery of service to the end user with less complexity.	Our current standard service management delivery model will be transformed to support heterogeneous services. This will be done as the various types of delivery model are included in the overall service, starting with the Cloud service provision of EDRM. We will retain control of the function while selectively outsourcing parts, such as Help Desk, that can be done more efficiently elsewhere.
Productivity (Standard) applications	The increasing need for better collaboration within the Home Office and across Government requires the ability to communicate efficiently with the right information. The productivity applications used in the knowledge industries has moved beyond email to include social media, contextual information provision and analysis of multiple large open data sets.	Through implementation of the Digital Strategy, we will start to make more use of Social Media as a way to communicate with the public and as a way of understanding the public response and usage of information provided. This will be provided alongside the current office automation, instant messaging and email functionality to provide a suite of options from which the most efficient tool can be chosen. The tools will be provided through commodity services.

Layer	Definition	How will the Home Office adopt it
LOB (line of business) or mission critical applications	LOB or Mission Critical Applications are those that deliver the actual service to the public. There is expected to be increased automation in delivery as the Home Office moves more to be a data driven Department. Such automation will support Home Office staff by carrying out more of the delivery process and freeing up resources within the Department.	We have a large legacy line of business estate that will need to be maintained. However, opportunities for change will be evaluated to ascertain if the applications can be replaced by commodity Cloud based services or by more flexible use or reuse of existing services. We will move to common definitions of capability and increasing use of common technology solutions.
Enterprise Applications	The Enterprise Applications provide the cross department intelligence and control. These are common to any large organisation and include such things as HR, Finance, Business Intelligence and monitoring of the effectiveness of delivery.	Given the commonality of Enterprise Applications across large organisations the move to common, shared services has been made in many departments. We have already made a large investment in Enterprise Applications through the adoption of the Adelphi model and will continue to do so, looking to use shared services and simplifying the business process to bring about a reduction in the tailoring of services. In time this will be a commodity service.
Common Applications / Components	Components or applications, usually modular and relatively small which are used across the Organisation, Line of Business and Productivity. This could include applications such as common authentication components or common distributed document management functionality.	We will look to re-use components across the application landscape. Where components are identified as being reusable across multiple types of applications they will become part of the shared application component list. The components will then be created in such a way as to allow easy reuse through the specification of easy to use interfaces or inclusion in standard design patterns. A library of common components will be developed and maintained centrally.
Data Integration	Joins up the information across the different delivery options	We will develop and use standards for Open Data and for Open API's that, not only allow but encourage a common view on the meaning of data and reuse of architecture for holding data. The ICW programme will initiate the data architecture and standards around the person, initially for the programme but also with wider organisational needs in mind.
Hosting	Hosting On Premise represents the traditional approach to hosting. Where the specialist nature of applications prevents their movement to Cloud there will continue to	The majority of the current service provision by us is using On Premise Hosting capability. We will seek to reduce the level of such hosting by moving applications to, in order of preference, public cloud, private cloud

Layer	Definition	How will the Home Office adopt it
	be a need for dedicated, On Premise, hosting. In general, this will be associated with legacy applications where the specialist nature or planned retirement makes investment in Cloud capability uneconomic.	or rationalised on premise hosting.
System Integration	Provides effective interoperability between services by allowing the different systems to communicate with each other and provides easier re-use across different services	As systems are increasingly delivered using multiple components and multiple vendors the integration will be vital to the delivery of a service to the user. Increasingly this will be identified as a separate activity rather than as part of the development and be an explicit part of the delivery, being provided by us as part of the project or through a specific contract.
PSN (Public Services Network)	The provision of network capability through a series of agreements to common standards, known data security constraints and interconnection agreements.	We will utilise PSN for network capability for projects and contract replacements and look to replace the current network contracts where cost effective. We will have a single network built on the PSN.

Home Office

The Home Office Technology Strategy is a Home Office policy document

Enquiries relating to this document should be addressed to:

Home Office IT

4th Floor, Seacole Building

Home Office

2 Marsham Street

London

SW1P 4DF

ISBN 978-1-78246-099-2 ***Home Office Technology Strategy***

In preparing this document, consideration has been given to the Home Office's legislative requirements for Impact Assessments including the Equality Impact.

In line with the Home Office Sustainable Development, this document is being distributed in electronic form.