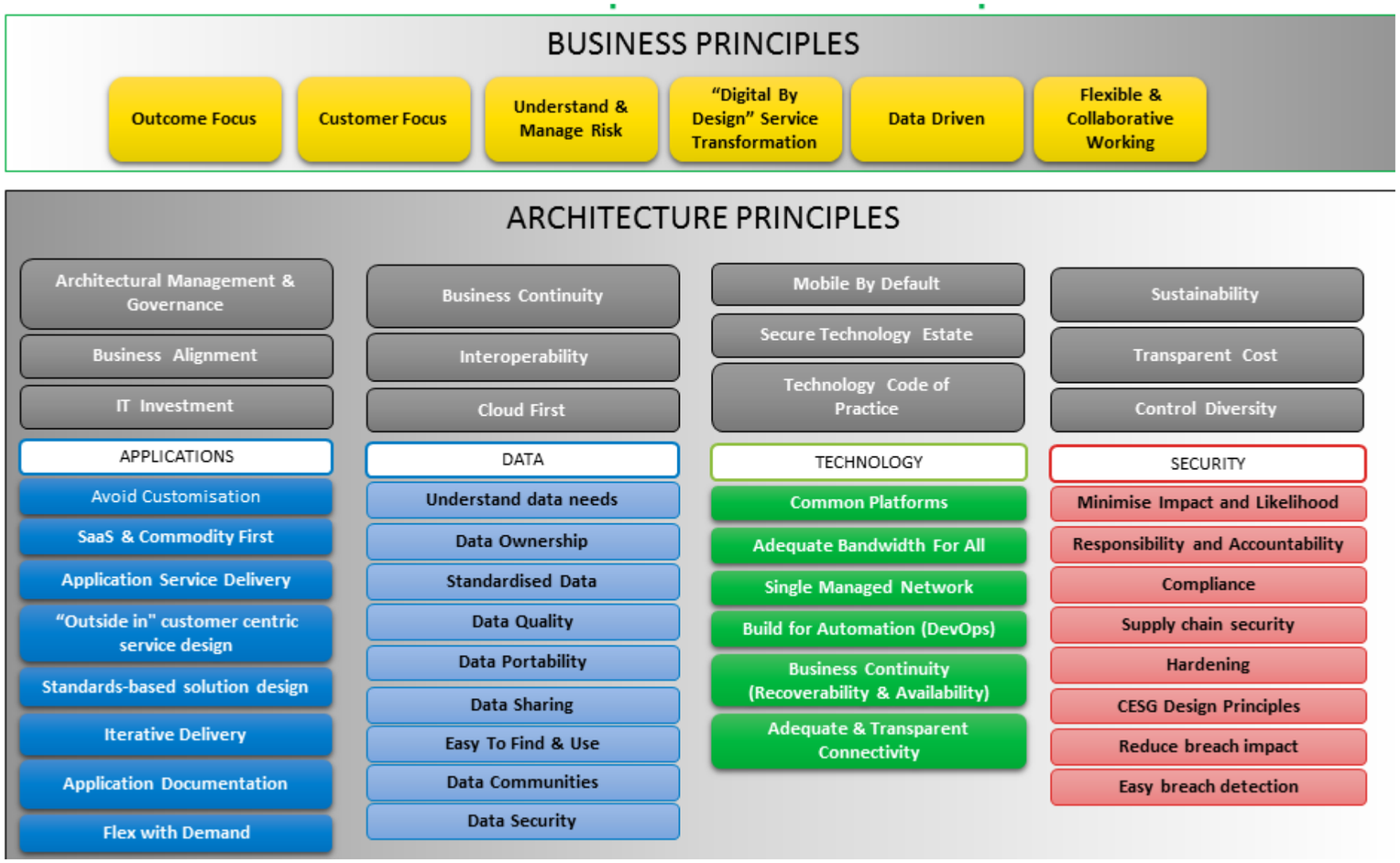
Defra Architecture Principles



Business Principles

ID	Name	Statement	Rationale	Implications	Source
BA_PRI_01	Primacy of Principles	These Principles of Enterprise Architecture management apply to all organisational units within the Defra group.	The only way we can provide a consistent and measurable level of Business/ICT alignment enterprise architecture management and governance in Defra is if all organisation units abide by these principles.	• Without this principle, exclusions, favouritism, and inconsistency would rapidly undermine the management of Defra's enterprise architecture. • Initiatives proposing architectural change will not begin until they are examined for compliance with the principles, and will be validated against the principles from inception to implementation. • These Enterprise Architecture Principles will be subject to continuous improvement and change control, and as such will be refreshed as required by any changes in Defra's business or technology strategy.	TOGAF 9 Specification / customised by SH
BA_PRI_02	Outcome Focus	We will be driven by outcomes, not solely by policy, and will realise outcomes through multi-stakeholder collaboration.	While we're constrained solely by policy we • cannot achieve sustainable cost savings • cannot innovate • cannot reduce administrative burden on UK business • cannot deliver streamlined end to end services as mandated by the UK Government Transformation Strategy.	We will • work with customers, third party organisations and across government agencies to deliver outcomes 'right first time', in the quickest, easy to use and cost-effective way. • challenge and change policy where necessary, to reflect opportunities to re-imagine and innovate. • will safeguard outcome focus through the application of standardised governance reviews of proposals, designs and solutions. • increase integration and co-ordination by developing consistent policy objectives, joining up planning and sharing processes, ICT and resources where appropriate. This will be underpinned by modern digital platforms and data, informing delivery planning and policy development.	Business Principles Workshops July 2016 / Defra Target Operating Model
BA_PRI_03	Customer Focus	We will be guided by our understanding of what our customers want to do when using our services, balanced with cost-effective delivery.	• Historically, our customer interaction has been driven by policy and internal processes, resulting in complicated customer journeys resulting in disengaged customers. • This approach drives increased cost and administrative burden for both the customer and government.	We will • engage with our customers digitally wherever possible whilst providing extra help to those who need it. • enable a service management approach • Enable streamlined interactions with customers (see also Outcome Focus Principle) • Practice continuous customer engagement to maintain effective services. • Be customer-focused, recognising the diversity of those we provide services for • Use data to monitor performance rigorously and ensure standards are met • Invite and act on feedback from customers	Business Principles Workshops July 2016 / Defra Target Operating Model

BA_PRI_04	Understand and manage risk	We will understand, accept and manage risk appropriately, on a case by case basis.	We need to • understand Defra business risks from all perspectives • establish whether risks are perceived or actual in order to reduce unnecessary mitigation cost • enable more efficient delivery of outcomes and business agility. • to accept the risk if the cost of risk mitigation exceeds the cost of the risk occurring • manage risk appropriately without stifling innovation.	We need a clear definition of Defra's risk appetite in order to innovate, challenge, redesign services and transform Defra as envisioned by the Defra strategy. • We will establish and strengthen a culture of innovation and ambition. • Defra is an outcomes-based organisation - we don't want to avoid risk: we want to embrace and manage it. • There are different kinds of risk. We are ready to accept more or less of it depending on the type of risk. We have: • Zero appetite for anything which would put our staff or the public at risk. • Low appetite for any risk to public funds (we have a duty to spend taxpayers' and charge payers' money well), our legal obligations (we must obey the law) or our reputation. • High appetite for the risks involved in thinking or working differently in order to deliver better for the people and places we serve. The kinds of risk we actively want to encourage include those involved in: • coming up with a different idea or policy • using novel technology • working with external partners.	Business Principles Workshops July 2016 / Defra Target Operating Model
BA_PRI_05	'Digital By Design' Service Transformation	Services will be designed/re-designed, built and delivered end-to-end to support Defra outcomes.	To deliver the outcomes, all elements of the service may need to change (e.g. Policy, Business, ICT, Data, Third Parties).	• We will redesign our services around the needs of our customers, only undertaking activity where it supports the delivery of our outcomes, and in a way that increases integration across the Defra group. • GOV.UK will be our information hub and the entry route to all of our digital services. • We will restructure our organisation in a way that best supports this service focus. • Digital will be our prime service delivery channel. • We need an organisational culture that - embraces change - challenges status quo - embraces collaborative service design • We need a clear understanding of what constitutes an end-to-end service. • We will make our services accessible, both internally and externally according to best practice. • All services will be delivered to agreed standards. • Service design will aim to maximise re-use of existing components to support business capabilities/activities.	Business Principles Workshops July 2016 / Defra Target Operating Model

BA_PRI_06	Data Driven	Defra will be data-driven, with our data being 'Open' by design and valued as a shared asset.	• Data supports real time analyses and decision-making for policies and services. • We have the skills we need to use data effectively and can access specialist services easily. • Our data can easily be developed into information at the scale we need to support decision-making. • Our data supports improved services for our customers.	• We will publish all our data unless there is a good reason not to and where we cannot publish data we will explain why. • We will collect, create and procure data once (Single version of Truth, regardless of where the data resides) to meet the needs of all internal users and this is shared widely across the group. • We will capture information once and use many times. • Defra's data will be seen as a valued government asset. • We will share data across Defra to facilitate joined up decision making and business outcomes. • We will make data easy to access for customers and employees alike where this aligns with our security principles. • ICT systems will enable the transformation of data into information and knowledge, allowing us to make better decisions.	Business Principles Workshops July 2016 / Defra Target Operating Model
BA_PRI_07	Flexible and collaborative working	We will enable the organisation to work flexibly and collaboratively to achieve Defra group outcomes.	In order to deliver Defra group outcomes, we need to work flexibly and collaboratively across Defra and in strategic partnerships with SME providers , supported by a Defra wide ICT architecture.	• We will aim to deliver external services from any device in any location to customers and employees alike. • Our mobile and laptop devices will work together to keep us organised and informed, using a range of collaborative applications and services. • We will maximise our ICT to do business in the most effective and efficient way for our people, be they customers or staff. • We will operate as a single organisation, with no technical boundaries. • We will seek to work flexibly in strategic partnerships with external SMEs to maximise our outcomes.	Business Principles Workshops July 2016 / Defra Target Operating Model

Enterprise Principles

ID	Name	Statement	Rationale	Implications	Source
E_PRI_01	**Architectural Management & Governance**	We will maintained a stream-lined, commoditised, business-aligned and cost effective architecture, managed and governed by a lightweight and tailored enterprise architecture framework.	Without effective and management of Defra's architecture we cannot • control cost and complexity of our technology estate. Technology sprawl and the inherent duplication of effort are counter-productive to government cost reduction strategy. • manage architectural risk arising from architectural decisions. This has direct implications on cost and quality of our services.	• We will need to ensure long term cost reduction, reduced complexity, improved value, quality and consistency by - controlling technical diversity - reuse of architecture building blocks - using common technology platforms - building repeatable patterns • We will produce, implement and promote an Architectural Management & Governance framework consisting of policies, principles, processes, people and tools. • We will establish a Defra-wide Enterprise Architecture governance structure, with clear Terms of Reference and accountabilities. All architectural decisions will be documented and traceable. • We will employ a software tool to manage architecture building blocks and artifacts and to provide relevant architecture views and viewpoints. • Architecture governance will be integrated with other governance frameworks in place at Defra, such as project/programme governance. • We will perform a formal assessment of risk before embarking on new technologies. This will be approved by the governance process.	SH
E_PRI_02	**Business Alignment**	We will practice strong alignment of IT execution with Business Strategy. • Our IT operating model will deliver IT services which support the achievement of corporate business plans and strategies, including our digital and data strategies. • Our architecture and design choices will make Defra responsive to business change.	• Defra is changing rapidly, as is technology. Our technology estate must be architected to be responsive to business as well as technology change. • The environment that enables access to services will be able to adapt to any business change requirements including organisation, role and group changes. • There will be a clear link between the delivery of the business strategy and delivery of the supporting IT business services. • Better understanding of business outcomes results in better IT delivery. • Keep business rules as simple as possible - • Analysts and architects must have the freedom to openly challenge business rules that are over complicated and potentially onerous.	• IT business services will support common business processes rather than be tailored to local business practice. This will require compromise and will facilitate business process rationalisation across the Defra technology estate. Business management of individual business services will need to operate within the cross-cutting portfolio framework. • Multiple legacy systems have been developed to closely match local business processes. These will be replaced with a rationalised set of IT business services that support common business processes. • Cross-cutting shared services will be proactively managed as a portfolio across Defra. The minimum number of shared services will support common business processes. • IT is involved at an early stage in business policy formation and planning. • Joint business and IT road-mapping and planning will be the norm. • There is clear linkage between business capabilities and the IT needed to support them, including whole life costs. • Management of IT business services is aligned with management of the business function they support (e.g. by business area). • Each IT business service has an executive custodian providing business ownership and accountability. • We will adopt the GDS model of challenging interpretation of legislation, rather than bespoking code as our default practice. • We will build for change - the environments, and the software that run in them, will be built only by using version controlled scripts. Code will be continuously integrated and will use automated tests to validate its quality prior to release. By investing our time in this, and the delivered capabilities of the cloud provider, we can take ourselves off the 'big bang' Technology Refresh treadmill and move to an incremental, continuous delivery model. The effort to set this up needs to be funded centrally.	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)

E_PRI_03	**IT Investment**	We will invest in key technologies, cost effectively, as required to enable and support the business.	• We will invest in IT based on the overall value provided by the investment. • Processes have to be defined to enable businesses to understand and use enabling technologies. • We will need to develop a better model to determine the value of IT to the business.	• We will not always choose the solutions with the lowest expenditure. • We will choose the solutions with the best value. We will leverage technology to automate and enable processes to ensure consistency, reliability and scalability. • We will actively develop a decommissioning plan for legacy applications. • There may be technical solutions which are possible when viewing technology as more of an enabler that are simply not considered possible with the current cost-focused mind-set. Examples of this "enabling" thinking in the current world might be SOA, Infrastructure virtualization, mobile device channels, etc. • We will apply the 80/20 rule which means if an Applications has 80% fit to a particular business requirements and the application is best fit for the architecture then that will be deemed “Good Enough”.	RPA Architecture Principles
E_PRI_04	**Business Continuity**	Enterprise operations availability, reliability and recoverability is commensurate with business criticality.	• Business operations and IT systems are inseparable. • System downtime directly impacts business performance. Business functions must be capable of recovery based on predefined SLAs in disaster scenarios. • There are few business processes that do not have a dependence on Information systems.	• Recoverability, maintainability & redundancy policies must be in place for all critical systems. • These policies will translate into operational SLAs that must be actively monitored. Recoverability, maintainability and redundancy requirements must be part of system design as key Non Functional Requirements (NFRs). • These NFRs must be tested before systems are rolled out to production. • Systems service management procedures must be made available for production rollout. • There will be a Business Continuity Plan with a dedicated section on systems disaster recovery.	RPA Architecture Principles
E_PRI_05	**Interoperability**	Software and hardware should conform to defined standards that promote interoperability for data, applications and technology.	Standards help ensure consistency thus improving the ability to manage systems and protect existing IT investments which will maximise RoI and reduce costs.	• The existing IT platforms must be identified and documented. • A process for setting, reviewing and maintaining standards as well as exception handling must be established.	RPA Architecture Principles V0.4

E_PRI_06	**Cloud First**	• We deliver cloud first, open, appropriate security, at minimal risk and offer services where they are needed most. • We will look to re-use existing commercial 'cloud' offerings first, rather than procuring dedicated hardware, as this will lead to cheaper and more flexible solutions.	We will achieve our strategic outcomes of cost reduction, flexibility, efficiency and change responsiveness by utilising the following benefits of cloud computing: • Elasticity - Resource in the Cloud can be freed and reserved flexibly, often within minutes. • Utility Computing - This model has the advantage of a low or no initial cost to acquire computer resources. • Standardisation - Variations in hardware are negated, because homogenous virtual hardware platforms are provided on top of them allowing virtual servers to migrate between multiple physical hardware platforms. • Time to Market - Cloud computing allows organisations to accelerate transformation programmes where change in the business is enabled by IT developments. • Scalability - Cloud services allow the business to baseline a normal capacity load and quickly vary that demand when necessary to protect them from performance issues. • Flexibility - Cloud computing provides the ability to auto-scale the infrastructure. • Simplicity - Management of an in-house capability requires a wide ranging lifecycle to be delivered, from architecture design, research, product solution and procurement, through to the implementation, configuration and management of the infrastructure across various levels including networks, security, back up administration and disaster recovery for mission critical data. Deploying into the cloud means that all these areas are part of the service levels agreed. • Cost - An outsourced cloud option avoids the need for upfront and ongoing capital expenditure to set up and maintain a viable IT infrastructure. Businesses going through transformation can make all of their project delivery costs OPEX as well as reducing the overall cost of ramping up development IT resource.	• We will minimise our network infrastructure by moving key elements to the cloud and simplify the remote user experience with always on VPN. We will manage a single IP address space for UC and future use • Defra will look to re-use existing commercial 'cloud' offerings first, rather than procuring dedicated hardware. • The order of preference for cloud services is SaaS > PaaS > IaaS. (Software/Platform/Infrastructure as a Service). Public Cloud > Private Cloud > CoLo > dedicated hardware in a private data centre. • We need foundation services to make this work, to ensure that people can log into them. • As we move into Cloud services we will need resource earmarked purely for monitoring changes in the products. • We will work more on integration. We care about external interfaces – so we may use proprietary standards internally. • Security controls should shift from devices to solution design and data handling. • Mobile users require an always on VPN with managed routes to trusted Cloud services. • Service suppliers should provide solutions that are compliant with commercial good practice standards to reduce the risk of threat to corporate services, lost or stolen data, malware and corporate reputation. • Print devices will be accessed via a cloud service that catalogues available devices and can direct print jobs to any Defra network printer from network connected user devices. • Keep it simple; one Cloud Proxy; one Cloud VPN & one Address Space • For those applications that have a business life beyond the current SI contract end dates, we will migrate those that we can to Cloud, based around their application patterns. Those that cannot be migrated will move to common hosting solutions. • Where new Systems of Record are required, commodity services will be deployed where possible. Commodity services will be Cloud based SaaS. • Defra Digital Transformation default procurement strategy is to use G-Cloud in order to provide IT solutions and only where the G-Cloud options have been exhausted will Defra CTO Leadership Team consider alternatives. Our IT solutions must withstand VfM challenge, allow agility (from a commercial and technological perspective), be scalable and commodity based IT-solutions. (commercial approach published August 2016).	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)
E_PRI_07	**Mobile By Default**	The right device, with the right apps, to get to the right data, where and when the user needs it.	• Our people will have the ability to work flexibly, from any location, using ICT that supports them in their roles. The ability to retrieve as well as update data in the field will enable them to respond swiftly to customer needs and in emergency situations. • Our mobile and laptop devices will work together to keep us organised and informed, using a range of collaborative applications and services. We will be able to change our services quickly and easily.	• Devices and solutions must support mobile working. They should be capable of being used independently of location e.g. within offices, between offices, at home or in the field. • Non-mobile solutions will be exceptional e.g. laboratories. • Devices and operating systems will be loosely coupled to services. • Mobile users require an always on VPN with managed routes to trusted Cloud services. • Devices and the application services they deliver will be capable of being changed or replaced independently. • We will design with choice and flexibility in mind: there will be many and different needs across the network so we will offer technology solutions that fit individuals and teams in the form of the "right" bundle of devices e.g. tablet/hybrid laptop/laptop & Smartphone. We will not deliver BYOD. • Device management solutions will be standardised and be independent of device suppliers. • Applications used on the estate will be managed through a catalogue – a combination of private appstores and white/blacklisting using native tools or MDM policies.	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)

E_PRI_08	**Secure Technology Estate**	Security and risk will be managed appropriately. Security should be "good enough" to mitigate identified risks and be nearly invisible to the user.	In order to mitigate risk and protect our data and technology, security must be pervasive across and through out the Business, Data, Application and Technology Architectures.	• We will secure all services and data at an OFFICIAL level with additional controls considered for OFFICIAL – SENSITIVE requirements. • All Defra Network users will have a single set of credentials to access all services on a need to know basis • Service suppliers should provide solutions that are compliant with commercial good practice standards to reduce the risk of threat to corporate services, lost or stolen data, malware and corporate reputation.	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)
E_PRI_09	**Technology Code of Practice**	Our ICT solutions (in so far as they fall into the GDS remit) will comply with the UK Government Technology Code of Practice published by GDS.	The stated aim of the Code is to ensure government technology • Meets user needs (based on evidence and research) • Meets key standards • Can be shared across organisations • Can be easily maintained and scaled • Isn't dependent on single suppliers	Please refer to the up-to-Date version here: https://www.gov.uk/service-manual/technology/code-of-practice.html	GDS
E_PRI_10	**Sustainability**	Our ICT solutions will adopt best sustainability practices, comply with relevant UK legislation, EU codes of conduct and international standards and contribute to and not detract from achievement of Defra Group's aims and objectives around sustainability	Compliance with and contributions to Government Greening Government Commitments, Greening Government ICT Strategy (as required by the GDS Tech Code of Practice), and Estates Rationalisation and TW3 programmes, Defra Group objectives for a cleaner and healthier environment protected against natural threats and hazards to preserve natural capital and biodiversity, comply with ISO14001 for Environmental Management, and achieve the Foundation Living Wage and EA's to achieve 20% reduction in the costs of sustainability impacts of its Supply Chain related to consumption of water, use of travel and paper and generation of waste	We need to assess sustainability risks and risks of consequential reputational damage for each ICT/Digital service arising from - asset construction - minimising use of critical materials - increase use of recycled materials - increase recyclability of assets - compliance with EU Labelling/GPP standards, and UK government buying standards (including Energy Star rating) - asset delivery - reduce use of packaging and resulting landfill - reduce GHG emissions from transporting goods to Defra sites - asset operation - ensure correct configurations and settings to achieve best environmental performance - asset recycling and disposal - sweat the asset until maintenance and support incur greater environmental impacts than presented by purchase of new assets across asset lifecycles - follow the Waste Hierarchy in recycling and re-using assets - minimise landfill resulting from disposal - fair and sustainable staffing arrangements for the service - adherence to the Equality & Diversity Act - adoption of best practices set out in the EICC and SA8000 standards	Unity/EA requirements as set out in UnITy sustainability strategy deck approved by NADB and Design Authority

Applications Principles

ID	Name	Statement	Rationale	Implications	Source
AA_PRI_01	Architectural Governance (Application Architecture)	Compliance to and evolution of the application architecture will be managed through controlled governance processes.	• Architectural change around our application estate needs to be tightly governed in order to remain business-aligned, cost-effective and risk-mitigated. • We need to control architectural decisions to prevent the random direction of IT growth, to reduce technical risk and achieve reuse.	• The Solution Architecture Assurance Board will regularly appraise solution designs against standards and Enterprise Architecture Principles. • Architectural Governance will guide the selection of and investment in application functionality. • GDS checkpoints will be part of the application design lifecycle (where the service falls under GDS remit). • Application and application service delivery will adhere to target architectures and reference models.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)
AA_PRI_02	Control Application Diversity	• We will control technology sprawl by limiting the number of applications that perform the same function. • Application proliferation will be controlled to minimise the cost of maintaining expertise in and connectivity between diverse technologies. • We will build re-usable components and in-situ services to generically service common needs.	• Reduce operational costs by having fewer environments and products to maintain. • Reduce the cost of future change by expecting simpler impact assessments and simpler migration/upgrade pathways. • Minimise the operational cost of maintaining many different assets in respect of vendor and contract management, support management etc.	• We aspire to a single application service to a common business need. • We need to engage with the marketplace and tailor our commercial approach to allow diversity to be constrained and reuse to be achieved and will use G-Cloud judiciously as a result. • All services that seek to introduce that introduce new applications or changes to existing applications must be supported by a sound business case which addresses the total cost of ownership of the application, plus any wider impacts on the application portfolio. • Application end of life will be anticipated, actively planned for and will be accounted for in whole life costs.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)

AA_PRI_03	Control Architectural and Technological Diversity	• Where it is necessary to build our application services we will constrain the diversity of the platforms, languages and toolsets they are composed of.	• Reduce the overheads of maintaining an unnecessarily wide range of skills and instead develop deep and sustained expertise in a subset of tools and languages appropriate to the services we need to deliver. • Improve the ability to create cross-functional teams and portable staff by reducing the learning curve to switch teams and respond to new business needs. • Reduce the complexity of future change by simplifying impact assessments and improving the repeatability of upgrades/maintenance due to a constrained problem set.	• Where we are required to operationally manage application services ourselves we aspire to use a manageable and cost-effective set of delivery languages, tools and platforms to deliver those application services. • We will follow standard target architecture patterns and standard target platforms to deliver services where they cannot be fulfilled by SaaS offerings. • We will progress our use of toolsets and versions in a controlled, best value and risk mitigated way, keeping up to date, but not "leading". • We will challenge the introduction of new platforms and languages on a benefits (right tool, right job), risks and costs basis and understand that if they are considered replacements a policy regarding replaced older technologies is in place.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)
AA_PRI_04	Avoid Customisation	We do not customise software	• Customisation is the most expensive way to modify software in the longer term. • Customisation is often avoidable by modifying expectations or ways of working.	• We will avoid customisation of software products directly. Where extension is absolutely required we will look to marketplace vendors for "plug-ins" as a first option and follow known and supported extension points and patterns that are supported through product upgrade only i.e. we will work alongside rather than customize in. • We will be open to change our ways of working and processes to avoid customisation of products. • In cases where customisation is deemed absolutely required we will understand the total cost of ownership for that customisation as per any other application delivery.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)

AA_PRI_05	SaaS & Commodity First	• We deliver SaaS services first. • We prefer commodity software to solve business problems	• The SaaS model is the most cost-effective way of delivering application services. • Mature SaaS solutions also deliver commodity benefits. • Commodities provide the best and most transparent value by providing utility based computing and reuse.	• Requirements/stories need to focus on need/outcome rather than on detailed changes articulating "how" something should be done to allow flexibility of tooling and removal/reduction of bespoke elements. • We will prefer SaaS offerings over other delivery options provided the approach does not close off sharing of data and reuse of services provided by cost-effective commodities. • We will be open to change our ways of working and processes to make best use of SaaS offerings and off the shelf products without customisation. • We will seek to reuse commodity based solutions to deliver application services or underpinning elements thereof.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)

AA_PRI_06	Application Service Delivery	We deliver application services as managed, loosely-coupled components.	• Loose coupling increases flexibility and reduces the impact of future business or technological change. • We need to improve the ability to reuse common services and leverage commercial products to respond to business need and change in a timely fashion. • We need to reduce costs associated with making and implementing system changes by only delivering the 'unique elements'.	• Reusable services and components will be catalogued and discoverable and have an onboarding mechanism and where required a centre of excellence team. • Application services will be exposed and secured using open standards. • Application services aspire to be agnostic of end user devices and end user operating systems. • A higher proportion of application services will be cross-cutting and utilised by more than one business service. Having no single business owner will highlight the need for strong change management and also utilisation tracking allowing cost apportionment. • Business services will be underpinned by many interacting application services. The operational management and support framework for that service set must be well designed, with clear responsibilities backed up by monitoring, diagnostics and management to meet business service levels appropriately.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)
AA_PRI_07	Accessibility	All of Defra’s applications should be designed or procured to be easily accessible to all users, including users who experience disabilities.	• This principle reflects Defra's commitment to make applications usable to all users, including those with disabilities, such as sight, sound or physical. We do not discriminate.	• Application services will meet as a minimum meet Level AA of the Web Content Accessibility Guidelines (WCAG) 2.0. • It will be recognised in some exceptional circumstances that measures other than a wholly technological solution may be the most appropriate to ensure discrimination of colleagues and customers does not occur.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)

AA_PRI_08	Applications will be delivered in the context of "outside in" customer centric service design	We provide applications that meet customer and business needs and that are responsive to changes and feedback.	• By designing for our customers we increase digital take up thereby increasing compliance and business efficiency. • By meeting the need we reduce the proliferation of grey IT and workarounds. • Designing to business needs and service functionality should lead to services designed around capability and lead to appropriate granularity of service provision.	• We must understand customer need that we are fulfilling and act on user insight evidence. • We must model the interaction between our business, the customer and the data and application services that are required to support that interaction. We will recognise that customers will utilise multiple services and seek synergy. • We must have resource in place (or service maintenance contracts) around application services that can change them responsively. • Applications will be architected to anticipate (but not design-ahead) future changes and minimize the impact and costs of that eventuality. • We will favour application tooling that provides "non development" change and improvement capability as it is the most responsive and least risk approach to responding to change. • We will ensure that we do not disenfranchise customers from interacting with our services due to technology, location, level of expertise or disability.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)

AA_PRI_09	Standards-based solution design	Our solution design will be guided by both industry and internal standards and best practice.	• By using standards and ideally open standards we maximise the ability for application components to interoperate cost-effectively and maximise the ability to purchase commodity components that will integrate, reduce need for bespoke elements and enable future low impact change. • By using industry and open standards we increase the talent pool of skilled individuals and suppliers who can quickly understand and work with our applications either as our resource or to leverage services we provide for exploitation and innovation. • By using standard patterns and services for known problem areas we reduce the cost of delivery by reusing existing products to accelerate delivery, reducing duplication and not rethinking already solved delivery problems.	• We must consider the industry support for products (application services, components, languages, platforms and tooling) that we select as ready availability of expertise and resource is a key contributing factor in driving down costs and maintaining a sustainable estate. It may sometimes be better to deselect "best of breed" in favour of "good enough and most readily understood and integrated". • We must ensure our architect and developer communities have an appreciation of agreed standards and patterns to be used is problem scenarios by creating reference materials and service catalogues with sufficient on-boarding support. • We will consider standards and patterns to be applicable to runtime, deploy time and design time artifacts covering concerns such as (for example) management and monitoring products and software defined architecture.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)
AA_PRI_10	Iterative Delivery	• We will evolve towards the right solution, delivering benefits early and often along the way. • Applications will be designed using proven design principles, methodologies and frameworks.	• There is a cost of delay that should be considered as a delivery driver and early delivery of minimum benefits may significantly offset these. • Delivery of minimum requirements is often sufficient and prevents the delivery of unnecessary "assumed" functionality. • Active delivery leads to practical learning, validates needs and assumptions re complexity, cost and user satisfaction and mitigates risk of erroneous "on paper" designs.	• We prioritise solution needs and consider requirements/stories fulfilment in terms of iterative delivery/release plans. • We pro-actively identify areas of technical debt adopted to facilitate early benefits delivery and plan for its replacement in future releases. • We make deliveries practical at the earliest opportunity to mitigate associated technical risks and validate and confirm the stated needs.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)

AA_PRI_11	Application Documentation	• As part of the initial provision of an application or service, there will be an agreed set of documentation produced. • During the life of this application or service, this agreed set must be maintained and will at any point in time reflect the actual deployed product.	• Documenting and modelling application services and their associated information (e.g. contract position, cost information) allows good quality impact assessment and estate management. • Documenting application services allows others to utilise and support them	• We ensure that our solutions, their composition, dependencies and usage information is documented to facilitate estate management (such as end of life planning) and to enable impact assessments in change situations (such as withdrawal of a dependency). • We ensure that any components and services created with an expectation of reuse have additional developer materials for enabling reuse and/or onboarding.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)
AA_PRI_12	We Deliver Application Services to Flex with Demand	• As part of application service delivery we identify any business, lifecycle or other demand patterns that would lead to require flex in capacity. • We design application services to scale flexibly both in a capacity sense and in a resilience and capability sense. • We recognise that it is often appropriate to scale only the high demand elements of a solution.	• Demand for services changes over time as new consumers are discovered, existing usage grows in demand and eventually as consumers move elsewhere during natural lifecycle management. • Many services have business patterns, such as annual renewal cycles or weather related demand which need to flex responsively. • Enabling services to scale responsively provides better value than paying for "peak demand" at all times. • Enabling services to scale at a component level is more cost effective than having to scale an end to end solution of which only part is in high demand.	• We ensure that the business demand profile that our solutions support is understood at the point of delivery and that it is monitored throughout the lifecycle of the service. • We make best use of cloud capacity models and design with flexible demand in mind for those services that will make use of it. • We identify high demand areas of the solution and potential pinchpoints and actively design composed solutions from components and services such that these may scale and grow independently.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)

AA_PRI_13	Transparent Costs	We deliver application services with transparent costs.	• Our services are apportioned between different budget holders and costs to support the IT estate they require should be transparent. • Understanding the cost of a service relative to the value it provides is key to estate management decision making. • GDS guidelines require that the cost per transaction is a visible metric for the service.	• Services that are pay by transaction must be technically capable of having costs apportioned to the service manager/budget holder. • The cost of shared components must be able to be apportioned to the supported solutions and business areas by splitting by transaction volume, user base or other recognised metric. Tagging and monitoring to achieve this must be available.	Workshops (Nigel Williams/Marian Zelman/Ben Sagar/Simon McDonald/Jacqueline Spencer)

Data Principles

ID	Name	Statement	Rationale	Implications	Source
DA_PRI_01	Understand data needs	Research to develop a deep knowledge of: the outcome, the data subject, potential users and their needs.	Acquiring and maintaining data is a substantial cost to Defra group, it also places a regulatory burden on our customers. It is only possible to express the data need if there is a strong understanding of the business outcome you're trying to achieve, the things you'll need to know, and potential users (our customers and our people) and their specific needs. Properly documenting needs will make it easier to identify if suitable data already exists.	Organisational implications ● We have a stronger understanding of why we need data and who uses it. ● To ensure costs are kept to a minimum data must only be acquired if there are clearly articulated data needs. ● Data will be defined for the widest possible group of users, for the benefit of the whole of Defra group. Technology Implications ● A clear understanding of data needs must be demonstrated before technology solutions are procured or developed. Key data lifecycle stages: You should consider all principles at each stage of the data lifecycle, but you must consider this principle more closely at the following stages: ● Need ✓ ● Check ● Obtain ● Store ● Share ● Use ● Archive	Collated from a number of sources by Andrew Newman, Data Policy Manager, Defra DDTS Data Programme

DA_PRI_02	Identify an owner for your data	All data must have a senior owner from the most relevant business area. The owner is responsible for ensuring the data is properly managed throughout it's life.	Data is an asset, it has a value to Defra because it enables us to make well informed decisions and provide services to our customers, we must ensure that these assets are adequately protected and properly managed. Clear data needs (see DA_PRI_01) enable us to identify how data supports our business objectives. It is therefore logical that data is owned by an appropriately senior individual in the most relevant business area.	Organisational implications ● Every dataset will have a named data owner, who will also be the 'Information Asset Owner'. ● The data owner will be responsible for ensuring the value of the data is maintained through good data management practice. ● The data owner will be an appropriately senior manager who: ○ Has the authority to make decisions and implement changes. ○ Can acquire and approve funding. ○ Is engaged in defining the strategy for their business area and hence the data needed. Technology Implications ● The data owner must be consulted on any changes to the data technology solutions that are used to manage it. ● The data owner must be kept informed of the initial and ongoing costs of technology solutions. Key data lifecycle stages: You should consider all principles at each stage of the data lifecycle, but you must consider this principle more closely at the following stages: ● Need ✓ ● Check ✓ ● Obtain ✓ ● Store ✓ ● Share ✓ ● Use ● Archive ✓	Collated from a number of sources by Andrew Newman, Data Policy Manager, Defra DDTS Data Programme

DA_PRI_03	Standardise your data	Using data standards ensure an agreed, repeatable way of formatting, configuring, using, inputting, quality assuring, holding, storing, outputting & transferring data	The opportunities to use data greatly increase when it is made available in standardised forms. A good data standard will help people understand: what the data is, how it is structured, it's quality, it's format and how it can be used. Researching and using existing standards will reduce duplication and differences between sets of data of the same type making them easier to use. Whilst benefit is gained from using organisational standards, much greater benefits can be realised by applying open standards.	Organisational Implications ● Data specialists can help business specialists to properly define data. ● Before defining a new standard check to ensure a suitable standard isn't already in use n Defra or doesn't already exist elsewhere. ● We are committed to using open standards where they exist and supporting the development of new, if possible open, standards where they don't. ● We have a consistent way of documenting our data and the relationships within it, ncluding: data models, vocabularies, formats, data quality. ● Our overall data integrity improves because inconsistencies and errors are eliminated with the result that our data becomes fit-for-purpose, confidence in our data improves and better decisions are made. ● Data linking and sharing is made easier and cheaper because of improved nteroperability. Data transfer effort and timeframes are reduced, IT integration is mproved and other organisations and the public can access and use our data more easily. ● Our level of compliance with mandated data standards (e.g. INSPIRE, WFD, FOI) mproves. ● Data reuse and exploitation opportunities are increased. ● The value of our data is increased. Technology implications ● Review existing data standards, create, update, govern and view, record and store in a single place to ensure they are used in our applications. ● When considering new technical solution proposals, the impact on the enterprise data model must be considered. ● Data standards must be produced during solution design and approved before development commences. ● As part of the solution assurance governance, impact analysis on the data model design must be carried out throughout development. Key data lifecycle stages: You should consider all principles at each stage of the data lifecycle, but you must consider this principle more closely at the following stages: ● Need ● Check ✓ ● Obtain ✓ ● Store ● Share ● Use ✓ ● Archive	Collated from a number of sources by Andrew Newman, Data Policy Manager, Defra DDTS Data Programme

DA_PRI_04	Understand and maintain the quality of your data	It is important to understand the quality of data and to understand if investment is required to improve the quality.	Good quality data enables good quality decisions. Getting data right first time helps us to save money. Data quality issues can have a big impact on the quality of our work and our reputation. Poor quality data can be expensive to fix or cleanse. The data's standard should define the quality requirements for the data (see DA_PRI_03).	Organisational Implications ● Data specialists will need to work closely with business specialists to regularly assess data quality against the relevant standard and maintain it's quality. ● Maintaining data quality has an associated cost that should be considered in data design and budget Technology implications ● Technology solutions must be designed to enable good data quality Key data lifecycle stages: You should consider all principles at each stage of the data lifecycle, but you must consider this principle more closely at the following stages: ● Need ● Check ✓ ● Obtain ✓ ● Store ● Share ● Use ● Archive	Collated from a number of sources by Andrew Newman, Data Policy Manager, Defra DDTS Data Programme
DA_PRI_05	Design to make data portable	Make your data easy to move between technology solutions and integrate from multiple sources.	Ensuring data can be easily separated from technology solutions enables those solutions to be changed without impacting upon the value or quality of the data.	Organisational Implications ● It will be easier to move between technology platforms as technology improves. ● The cost of moving data between systems will be reduced Technology Implications ● The impact of ICT changes on data must be assessed before the change is made. Key data lifecycle stages: You should consider all principles at each stage of the data lifecycle, but you must consider this principle more closely at the following stages: ● Need ● Check ● Obtain ● Store ✓ ● Share ✓ ● Use ● Archive	Collated from a number of sources by Andrew Newman, Data Policy Manager, Defra DDTS Data Programme

DA_PRI_06	Share your data as widely as possible	We are an open data organisation, we must share our data as widely as possible. You must ensure there are no barriers to sharing your data between Defra group bodies.	We want as many people as possible to be able to access and use our data to create a great place for living. Opening up our data enables others to use it to inform and build their businesses and enables others to use it to do the things we can't. Opening up our data also buildings trust, transparency of the data we use to make decisions allows others to hold us to account, building trust in government and providing the potential to improve the way we do things.	Organisational Implications ● Data sharing agreements and consents may be needed to allow Defra group bodies to share data between themselves without restriction. ● Data must be published under an open licence, such as the Open Government Licence (OGL), by default. Where this is not possible the data must be published using the most open way possible. ● You should consider the risks associated with making data open. Technology Implications ● Technology solutions must be designed to enable the open publication of data. Key data lifecycle stages: You should consider all principles at each stage of the data lifecycle, but you must consider this principle more closely at the following stages: ● Need ● Check ● Obtain ✓ ● Store ● Share ✓ ● Use ● Archive	Collated from a number of sources by Andrew Newman, Data Policy Manager, Defra DDTS Data Programme
DA_PRI_07	Make your data easy to find	t's essential to make it easy for users to find your data, understand it's quality, how t was made, and how it can be used.	We want as many people as possible to be able to access and use our data to create a great place for living. Making your data findable will enable others to find and use t, reducing the risk we will spend time and money acquiring similar data multiple times and enable good data management. Being able to easily find data will decrease the time we spend responding to requests for information. It will also improve the likelihood we use the same source and therefore provide consistent answers to customers from across the Defra group.	Organisational Implications ● All data must be described using standards compliant metadata. Technology Implications ● Metadata should be maintained alongside data and made available to a central metadata service. Key data lifecycle stages: You should consider all principles at each stage of the data lifecycle, but you must consider this principle more closely at the following stages: ● Need ● Check ● Obtain ✓ ● Store ● Share ✓ ● Use ✓ ● Archive	Collated from a number of sources by Andrew Newman, Data Policy Manager, Defra DDTS Data Programme

DA_PRI_08	Make your data easy to use	Your data must be made available, where possible from source, in easy to use formats and if feasible in linkable forms.	We want as many people as possible to be able to access and use our data to create a great place for living. The easier Defra data is to use the more likely we will be able to realise the benefits of sharing data across the group, achieving efficiency savings. We want others to use our data to achieve more for the environment the economy and society - the more accessible, reliable and usable Defra data is, the more likely we will achieve these aims. Promoting use of data will reduce data duplication and reduce the costs of data capture and hosting. Our work to make certain data available as Linked Data has shown that further value can be unlocked when information is made available in a form that can be linked.	Organisational Implications ● Making data easy to use may lead to additional costs, however these should be offset by the benefit of using data others have made open and reusable. Technology Implications ● Data will be managed and accessed from source where possible. When not possible data will be mastered but the source and update cycle will be clear from the data inventory. ● The use of API's registries and web services, will generate authoritative sources of data that must be used across multiple ICT services. ● The use of linked data methods must be fully considered. For example the use of unambiguous identifiers (EG URIs), classifying items and the relationships between them, and linking of items. Key data lifecycle stages: You should consider all principles at each stage of the data lifecycle, but you must consider this principle more closely at the following stages: ● Need ● Check ● Obtain ● Store ✓ ● Share ✓ ● Use ✓ ● Archive ✓	Collated from a number of sources by Andrew Newman, Data Policy Manager, Defra DDTS Data Programme
DA_PRI_09	Build a community around your data	Build a community around your data that includes the data owner, data managers and users. Seek feedback from this community and act to improve the data in response.	Building a community around your data will enable you to continuously ensure the data meets the business needs. It will also enable you to continuously test the identified needs are correct and current.	Organisational implications ● The data owner must be empowered to respond to feedback from the community. ● Data needs can constantly be reviewed. ● Understand who can make what decisions Technology Implications ● Technology providers should participate in the community and respond to feedback from the community. Key data lifecycle stages: You should consider all principles at each stage of the data lifecycle, but you must consider this principle more closely at the following stages: ● Need ✓ ● Check ● Obtain ● Store ● Share ✓ ● Use ✓ ● Archive	

Technology Principles

ID	Name	Statement	Rationale	Implication	Source
TA_PRI_01	Architectural Governance (Technology Architecture)	Compliance to and evolution of the infrastructure architecture will be managed through controlled governance processes.	• Architectural change around Defra's infrastructure needs to be tightly governed as we move from two incumbent suppliers to a multi-supplier model. • We need to control architectural aspects of procurement decisions to prevent the random direction of IT growth, to reduce technical risk and achieve reuse.	• Architectural governance will be applied by a combination of the Service Strategy & Design Steering Group (SSDSG), the Defra Design Authority and the Unity Delivery Board. • We will operate a defined and documented approval process around all UnITy 'Inbound and Outbound' architectural artifacts, which will encompass validation against these Enterprise Architecture Principles.	SH
TA_PRI_02	Control Infrastructure Diversity	Technological diversity is controlled to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.	• Reduce / minimise cost of IS/IT Infrastructure. • Minimum technical diversity allows for - standard packaging of components; - predictable implementation impact; - Minimum skills & expertise required; - Reduced testing - Increased flexibility to accommodate technological advancements - Better control over technical administration and support costs - Reduced Interfacing / integration requirements - Improve leverage with selected vendors.	• Policies, standards and procedures that govern acquisition of technology must be based on this principle. • List / set of preferred technologies (Technology Strategy) will have to be selected and approved. • Some constraint will be put on technology choices. • Process for evaluating new technology and evolving existing technology set to meet evolving requirements will have to be developed. • All solutions must be evaluated against existing skills, competencies and standards.	RPA Architecture Principles V 0.4

TA_PRI_03	Common Platforms	By default we share common platforms and ways of working across the network.	• To get best value for money Defra needs to make sure we work together to only deliver and maintain services once for Defra, rather than having the cost of creating and maintaining multiple services that do the same thing. • Many service needs are similar across the Defra Network and economies and cost savings can only be made by sharing tools and costs. • Our technology will enable our customers and users to work as 'one business'.	• We will use common device management platform(s) • We will exploit common platforms, within the Defra Network and more widely across government. • To obtain best value for money IT support, common component services need to be managed as a cross-Network portfolio. • IT plans and work will be coordinated across Defra. We will have processes to spot commonality, to prevent duplication and to actively support sharing. • Multiple legacy systems have been developed to closely match local business processes. These will be replaced with a rationalised set of IT business services that support common business processes. • Active portfolio management will be an on-going resource demand. • IT business services will support common business processes rather than be tailored to local business practice. This will require compromise and will facilitate business process rationalisation across the Defra Network. Business management of individual business services will need to operate within the cross-cutting portfolio framework. • Active portfolio management will require strong governance. • Hosting needs to be configured in such a way as to support service separation (from a monitoring and charging perspective) while still re-using as much common infrastructure as possible.	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)
TA_PRI_04	Adequate Bandwidth For All	As far as is reasonable, no user or location will be without coverage.	This principle underpins and is essential for our Enter-prise wide principle 'Mobile by Default'.	• We will increase coverage to sites and remote users by providing a dedicated 2Mbps per FTE by 2019.	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)

TA_PRI_05	Single Managed Network	A Single Managed Network Connecting all Major Sites, with Site Network Resilience Only Where Required.	End-to-End monitoring is vital for service management and efficiency.	• There will be a single MPLS network for the whole of the Defra Network augmented, if necessary, by direct Internet access. • True network resilience will be focussed on the key sites (HQ and emergency). • We will have real-time end-to-end monitoring and analysis of the network. • We will deliver an aggregated, single interface to deliver end to end monitoring across all Defra Network services. •We will deploy a test toolkit that supports all elements of testing requirements including security We will deploy a single architecture toolkit that delivers a common set of standards, blueprints and configurable items across the Defra Network • We will deploy a single architecture toolkit that delivers a common set of standards, blueprints and configurable items across the Defra Network	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)
TA_PRI_06	Build for Automation (DevOps)	• The environments, and the software that run in them, will be built only by using version controlled scripts. • Code will be continuously integrated and will use automated tests to validate its quality prior to release.	By investing our time in this, and the delivered capabilities of the cloud provider, we can take ourselves off the 'big bang' Technology Refresh treadmill and move to an incremental, continuous delivery model. The effort to set this up needs to be funded centrally.	• Automated tests will need to be built into applications early on, in order to support this continuous integration/continuous deployment model.	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)

TA_PRI_07	Business Continuity (Recoverability & Availability)	We will deliver a Defra Network incident response & disaster recovery & business continuity approach. Our services are consistent with our roles as critical incident responders.	• To enable Business Continuity / Disaster Recovery we will deliver a consolidated end to end incident response environment that supports the Defra Network. • Cost savings through organised rapid response to incident management, and through resuming operations without too much disruption. • Avoidance of public embarrassment and reputational damage.	• Where we need resilience we will look at multiple services. • We will deliver a consolidated end to end incident response environment that supports the Defra Network DR & BC operating models • Device management solutions will be standardised and be independent of device suppliers. • Resilience and DR are design features, not bolt-ons. Resilience during incidents requires more than one solution to be in place for some. • Establish an incident response DR capability, and provide training and regularly test it. • Implement end to end resilience of critical services. • HQ and emergency incident management sites will get true end-to-end resilience across symmetric links. • Where divergent routing is required, but not possible, we will provide 4G access to MPLS. • Product evolution and consolidation will be an ongoing challenge. • Device policies need to be agreed that achieve a balance between business requirements and risk (CESG guidance). The likely result will be a Windows solution and a Smartphone solution with a degree of overlap e.g. tablets. • As a critical incident responder, we will look to capitalise on hosting used by other such organisations, rather than building the entire infrastructure ourselves. • Cloud based tools may not have what we consider Gold level availability standards.	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)
TA_PRI_08	Adequate & Transparent Connectivity	As far as is reasonable • customers and staff will be able to connect to our networks regardless of user or network location. • a single managed network will connect all major sites, with site network resilience only where required. • no user or location will be without coverage.	End-to-End monitoring is vital for service management and efficiency.	• Wireless access is the default access method • We will crack the issues preventing direct wireless access to the LAN. • New buildings will be wireless only. • Outside of the office we will enable access to public wifi hotspots. • The full range of device connectivity possibilities will be used balancing speed/cost	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)
TA_PRI_09	Common Availability levels	**TO BE COMPLETED**	•Standard hosting will be predicated on the minimum number of servers for each function to support the required workload. •Process critical – will include resilience •Business Critical will include geo-replication of the services, using the provider's native capabilities. •Life Critical services (Flood response related) will require further augmentation	**TO BE COMPLETED**	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)

Security Principles

ID	Name	Statement	Rationale	Implications	Source
SA_PRI_01	Secure Technology Estate	Security and risk will be managed appropriately. Security should be “good enough” to mitigate identified risks and be nearly invisible to the user.	Drive from Cabinet Office for Good Enough security and to not over engineer solutions and security	• The Defra Network will secure all services and data at an OFFICIAL level with additional controls considered for OFFICIAL – SENSITIVE requirements. • All Defra Network users will have a single set of credentials to access all services on a need to know basis • Service suppliers should provide solutions that are compliant with commercial good practice standards to reduce the risk of threat to corporate services, lost or stolen data, malware and corporate reputation.	UnITy principles, High-level Defra Principles (June 2015, NaDB), Guard Rail Objectives (Dave Williams)
SA_PRI_02	Minimise Impact and Likelihood	Our infrastructure and cloud services will adopt clear measures to minimise the likelihood and impact of any security incidents	Avoidance of public embarrassment and reputational damage.	• Proportionate response: Security measures should be proportionate to the threat. • Goal-based security: As a general principle, we shall favour goal-based security. This means that a security and assurance level is set that the market is expected to comply with. • Designed-in security: The Programme must consider cyber security from concept and development onwards.	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles and HMG Security Policy Framework
SA_PRI_03	Responsibility and Accountability	Our people will have clearly defined responsibilities to protect our data, technology and services according to government standards	Ensure the responsibilities arrangements for the system are clear	• When implementing security there is a natural tendency to focus the majority of effort on the technological elements. • Although important, technology is insufficient on its own to provide robust protection. It is essential that people operate best practice.	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles and HMG Security Policy Framework
SA_PRI_04	Compliance	We will process and store our data in compliance with government standards	Ensure the compliance arrangements for the system are clear	Non-compliance with respective legislation could have serious reputation, legal and financial ramifications	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles and HMG Security Policy Framework

SA_PRI_05	Governance	● We will implement effective control over the security of the service and of the data held, not blindly follow pre-determined processes. ● We will consider the cost of not doing something just as much as the cost of doing it. ● There will be no ambiguity about responsibilities. We will ensure that the right people are empowered to protect the service. ● Where trades need to be made between security, usability and cost, we will agree those trades in terms of business impact rather than in technical language.	● Ensure the governance arrangements for the system are clear. ● Make it easy for everyone involved in designing and operating the service to know what their role is, and what constitutes acceptable behaviour.	● We will risk assess the controls we believe to be proportionate, otherwise the Programme will likely procure expensive and ineffective technologies. ● Proportionate response: Security measures should be proportionate to the threat. ● Goal-based security: As a general principle, we shall favour goal-based security. This means that a security and assurance level is set that the market is expected to comply with. ● Designed-in security: The Programme must consider cyber security from concept and development onwards.	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles and HMG Security Policy Framework
SA_PRI_06	Supply chain security	● We will use suppliers to help build and operate a service and ensure that they understand that they play a vital role in keeping it secure. ● We will be clear about intentions and requirements for security in contracts with suppliers. We will not to be too over-prescriptive to prevent this leading to adversarial behaviour. ● We will build a shared risk proposition with suppliers so they are invested in doing the right thing, as well as supporting the contract. ● Our suppliers will secure our services to maximise our resilience against attacks. ● The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.	Understand the role the suppliers play in securing your service	If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles and HMG Security Policy Framework
SA_PRI_07	Technology - Hardening	We will build in protection against common attacks.	Making services hard to compromise	● Cyber security must be considered as an integral part of our general security package. ● Protect: Installing specific protection measures to prevent and discourage cyber attacks against systems ● Detect: Establishing mechanisms for rapidly identifying actual or suspected cyber attacks ● Respond: Undertaking appropriate action in response to confirmed security incidents against systems	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles and HMG Security Policy Framework

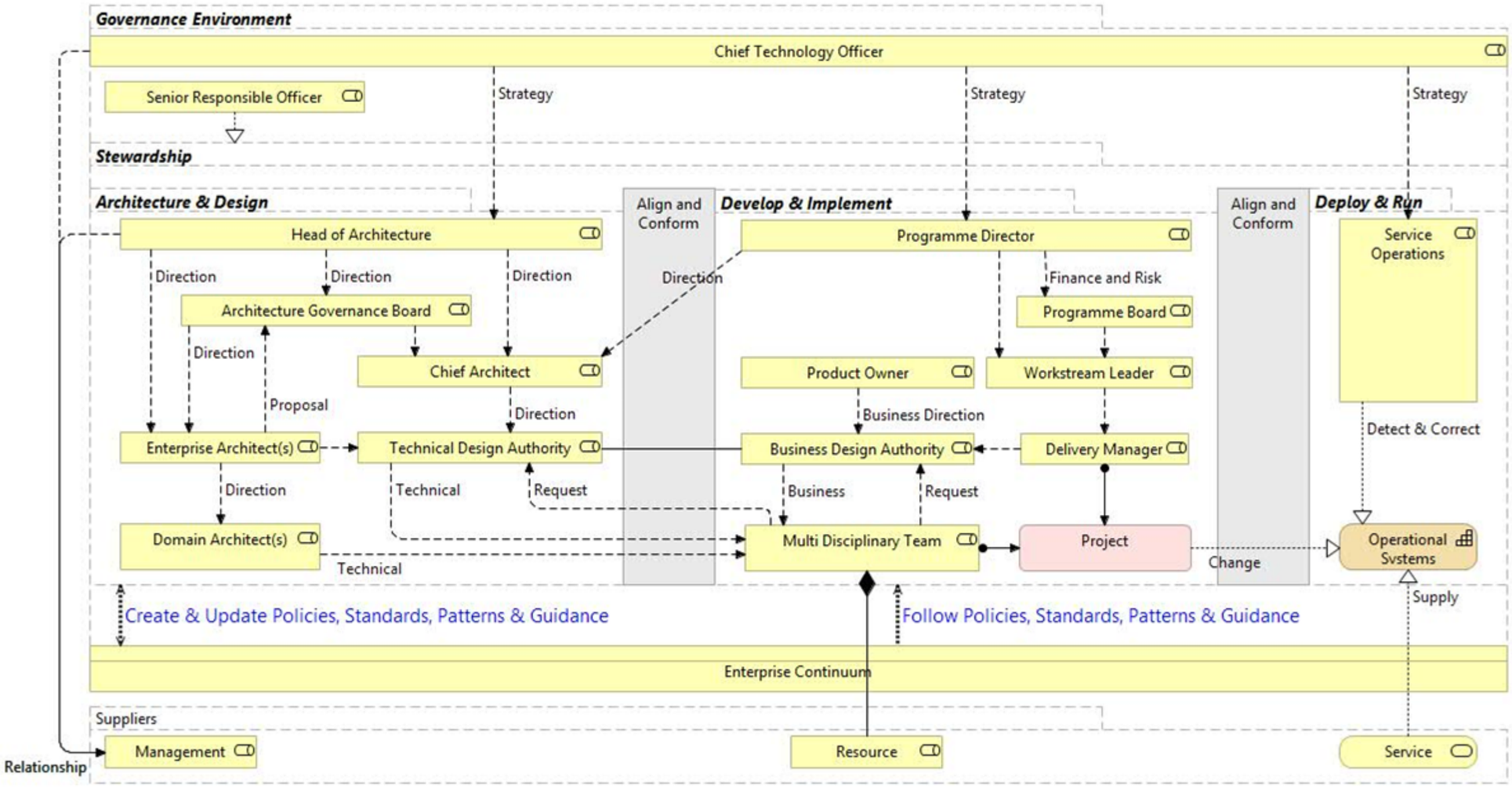
SA_PRI_08	Technology - NCSC Design Principles	We will use NCSC security design principles to help us consider which concepts and techniques we would use to make it harder for attackers to compromise the service whilst implementing commodity products.	Making services hard to compromise	Constructing a security framework for any system is not just a matter of deploying protection measures. It is important to be able to detect possible attacks and respond in an appropriate manner in order to minimise the impacts. Technical, procedural and managerial protection measures When implementing security there is a natural tendency to focus the majority of effort on the technological elements. Although important, technology is insufficient on its own to provide robust protection. It is essential that people operate best practice.	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles, https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main and HMG Security Policy Framework
SA_PRI_09	Technology - Reduce breach impact	We will minimise the impact of any successful attack. We will use NCSC security design principles to help us create services which naturally minimise the degree of any compromise.	Reducing the impact of a compromise	Constructing a security framework for any system is not just a matter of deploying protection measures. It is important to be able to detect possible attacks and respond in an appropriate manner in order to minimise the impacts. Technical, procedural and managerial protection measures When implementing security there is a natural tendency to focus the majority of effort on the technological elements. Although important, technology is insufficient on its own to provide robust protection. It is essential that people operate best practice.	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles, https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main and HMG Security Policy Framework

SA_PRI_10	Technology - Easy breach detection	We will implement system monitoring to enable operations to spot an attack when it begins and analyse and respond to the attack while it is underway. In the short term, we will disable functionality or scale computing resources if it is the only viable option available to prevent any escalating threat. We will use NCSC security design principles to help us deliver services that make compromises easy to detect.	Making compromises easy to detect	● Constructing a security framework for any system is not just a matter of deploying protection measures. It is important to be able to detect possible attacks and respond in an appropriate manner in order to minimise the impacts. ● Technical, procedural and managerial protection measures ● When implementing security there is a natural tendency to focus the majority of effort on the technological elements. ● Although important, technology is insufficient on its own to provide robust protection. It is essential that people operate best practice.	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles, https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main and HMG Security Policy Framework
SA_PRI_11	Technology - Cloud	● We will use cloud hosting providers preventative measures to reduce the impact of malware attacks. ● We will be aware that the security properties of cloud services can vary greatly and will use NCSC Cloud Security Principles to help us consider the significant security properties of services when choosing which to use.	Host in the Cloud	● Service providers must maintain systems throughout their life cycles to ensure optimum functioning. They must keep abreast of new developments in malware and other threats, through engagement with organisations such as NCSC, NCSC, CPNI etc. ● Any Service providers who cannot comply with our requirements and industry best practice will be 'frowned upon' and additional assurances will be required	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles, https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main and HMG Security Policy Framework
SA_PRI_12	Information/Data - Service Design	● We will document a clear understanding of the purpose of the service. ● We will define what data is required to deliver the service and what level of data protection is needed ● We will take account of every possible point at which data could be stored, processed and rendered including end user devices, networks, 3rd party services and copies of data.	● Understand the service and the data we will need to operate it ● Ensure a clear, end-to-end understanding of the service and how it is accessed	A service that is poorly designed and understood is likely to not be fit for purpose	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles and HMG Security Policy Framework
SA_PRI_13	Information/Data - Processing & Storage	● We will understand the difference between processing and storing data. ● We will not habitually store all data that is captured unless it is necessary for later retrieval. ● We will establish data retention and removal policies	Only handle data which is essential to the service	By handling data that is essential to the service, we can reduce the impact of a compromise, but also foster good behaviours in storing only what is necessary	Unity/Defra Security Principles (Phil Derbyshire) Cloud Security Principles and HMG Security Policy Framework

Evergreen Principles

ID	Name	Statement	Rationale	Implications
EG_PRI_01	Keep Evergreen	All new IT services & devices will be kept on the latest patch of supported versions of software.	Technical debt introduces security risks and inhibits business change. Given the last publicised cyber-security breaches were diagnosed as being the result of unpatched middleware, we cannot be the next victims, especially during the EU Exit negotiations.	While the software in use doesn't need to be the latest release, it must be supported. Where software provides the capability to self update, we must find a mechanism to support that capability, without unnecessarily introducing service risk.
EG_PRI_02	Design for Decomposition	New services should be designed such that one functional component can be swapped out for another comparable product with minimal investment.	Many of our existing services are heavily interfaced to each other, and to uplift one component we have to uplift a lot more. By designing future services differently, we can ease that ability to migrate.	Decompose future services as far as possible in order to ease migration from one product to another. Adopt Open Standards as far as possible. (probably covered by a different principle elsewhere).
EG_PRI_03	Design for Automation	In order to ease the maintenance of a service, the build of the components should be scripted as far as possible, including automation of testing.	In order to keep all parts of a service within manufacturer support, it is necessary to regression test key components against all updates. Automated delivery pipelines need to be the ambition to help speed up the delivery processes.	Build the automation pipelines before building the services, as far as possible.

Technical Governance



- The **Architecture Governance Board** meets monthly (or by exception) to agree standards, patterns and exceptions, and review peices of work throughout their lifecycle. **See also AGB ToR**
- The **Chief Architects** for each programme ensure that work meets standards or is managed as an exception.
- **Enterprise Architects** lead the development of standards and patterns, in partnership with programmes, and ensure programmes work together.
- **Domain Architects** lead the work on any given area, especially of technology.

Common Technology Choices

Technology	Position
Agile Delivery Management	-Jira -Trello -VSTS
Prototyping	TBC
Service Design	TBC
Development Languages	-Node.js using Hapi for new online Digital Services -C#.Net to extend commodity platforms (.Net Core wherever possible)
Code Version Control	-Consolidate on Git -Defra GitHub for all open code -Private GitHub, GitLab and VSTS Git
Hosting	-Cloud First. Azure (preferred) and AWS (where specific native AWS services are needed) as provided by Defra Cloud Hosting
Integration Platform	-Always look at Dell Boomi first for integration options assessment -Local AWS and Azure facilities where strong technical fit
Application Databases	-RDS and Azure PostgreSQL -SQL Server -Azure Cosmos DB (interim NOSQL solution)
Continuous Integration	-Jenkins and VSTS -Various online tools for open code verification
Test Management Tools	-Jira and VSTS
Automated Test Tools	-JMeter, Selenium and Cucumber -SonarQube -Browserstack -Various free online tools
Service Analytics, Service Monitoring and Management	-Google Analytics -LogicMonitor -ServiceNow
Customer Platform (CRM)	-Dynamics 365
Other Common Platforms	- Defra.identity platform for customer Identity & Access Management