PRINCIPLES

Digital, Data and Technology (DDaT) Design Authority

Version 2.0

Date: 5th July 2018

TABLE OF CONTENTS

PURPOSE

This document contains the principles the IT Architecture of the BEIS DDaT Organisation.

Architecture principles, policies and standards provide generic statements which are used to inform the overall architecture of an organisation. These statements are applied when making decisions about solutions and technology investments. They are written in alignment to Government Digital Services (GDS) statements and where these diverge from GDS the reasoning for this will be outlined.

It is easy to think about principles, policies and standards as a single thing, below is a brief outline of the differences between each of them.

WHAT IS A PRINCIPLE?

A set of high-level statements that are intended to rarely change, setting out how an organisation goes about fulfilling its mission[1]. These generally include the statement, the rationale and the implications. As an example, GDS identifies "Cloud native" as a principle stating "include the flexible adoption of Software as a Service (SaaS) applications, which are often loosely coupled and quite task specific."[2]

PRINCIPLES

Architecture principles are outlined in this section. Each principle has a name, statement, rationale and implications[3]. This structure provides clarity on what the principle is, why it has been incorporated and what are the ramifications.

Architecture principles tend to be similar between organisations as such these have been adapted from other sources were possible.

[1] http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap23.html

[2] https://governmenttechnology.blog.gov.uk/2017/02/03/clarifying-our-cloud-first-commitment/ https://governmenttechnology.blog.gov.uk/2016/09/13/we-are-renewing-our-cloud-first-commitment/

Principle 1. Cloud Native

Cloud-Native

Potential public cloud services will be evaluated before considering alternatives.

Rationale

This is an alignment to the GDS "Cloud Native" (previously "Adopt cloud first") principle as part of the GDS Technology Code of Practice[4]. Independent of the GDS principle, the {organisation name} has an intention to reduce the on-premises infrastructure to improve efficiency, reduce costs, and accelerate project delivery. Cloud-based solutions will also provide operational improvements in reliability, performance and automation and it is important that these aspects are considered as part of any cloud selection process.

Overall, there is a trend in industry to adopt cloud solutions to deliver business capability, rather than hosting on-premises. For "normal" workloads it is generally cost-effective to use cloud solutions rather than hosting on-site.

The type of cloud solution (SaaS, PaaS, or IaaS) is covered in a separate principle. Additionally, the original GDS Cloud First principle includes a statement relating to value for money which is also covered as a separate principle.

Implications

Technology decisions should avoid solutions which do not progress towards a cloud-based hosting model. This means that solutions should either be on public cloud or to support the move to public cloud.

Tactical solutions running on-premises are acceptable if they have a defined lifetime and/or plan to move to cloud in the future, however, ideally, should be avoided as they generate technical debt.

Principle 2. SaaS before PaaS, PaaS before IaaS

SaaS before PaaS, PaaS before IaaS

When choosing cloud solutions, Software as a Service (SaaS) should be the first preference, followed by Platform as a Service (PaaS) and finally, Infrastructure as a Service (IaaS). This forms an extension of the original "buy-before-build, configure-before-customise" principle. Within each of these "aaS" tiers, any government-based cloud offering should be considered first to ensure alignment to GDS and simplify procurement and management.

Rationale

When leveraging cloud solutions, it is generally better to choose solutions which offer the highest level of out-of-the-box capability and management (assuming business requirements can be met). As

[4] https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

the choice moves from SaaS to PaaS, and PaaS to IaaS there is additional effort to both build and maintain the solution as more of the solution is configured or customised.

IMPLICATIONS

Generally common business services such as HR and Finance should be SaaS-based as these are common to most organisations and have similar requirements. There may be some need to slightly change business processes to fit within the chosen solution however this is a worthwhile investment to reduce the total cost of ownership of the solution.

PaaS provides a good solution for unique business components (such as xxx, yyy, zzz and xzy) as the platform is fully-managed and the business specific functionality can be built/configured on top of the platform.

IaaS provides a good temporary solution for "lift and shift" models as part of a migration to cloud but does not offer significant benefit to on-premises management (assuming there is still infrastructure located and operating on-premises).

Principle 3. Value for Money

VALUE FOR MONEY

Solutions will be evaluated and selected with a commercial view of the solution ensuring that the proposed solution offers value for money.

RATIONALE

The original GDS "Cloud First" principle includes a statement that non-cloud options must represent best value for money. This principle extends on the GDS one to encompass both public cloud and on-premise solutions as it is important to consider value for money no matter the underlying implementation.

It is important to ensure that any proposed architecture includes an understanding of the full life cycle (investment and operational) cost implications to inform current and future funding needs.

IMPLICATIONS

It should be noted that value for money does not mean the cheapest solution. Value for money should also consider the functionality being delivered as well as the initial and ongoing cost of the solution. This should also be considered within a realistic estimate of the useful life of the solution. Ongoing costs should include support, maintenance and hosting costs as well as any continuous improvement activities that are expected. This is to ensure a complete view of value is obtained, e.g., while a product/solution might be cheaper to complete the initial installation, ongoing work on the product/solution may become cost prohibitive due to access to resources in the market, effort to make changes etc.

Where possible common comparators should be used to evaluate the pricing component of value for money (e.g. if buying storage, use cost-per GB). This should form part of an appropriate procurement process to evaluate the solution considering the overall value.

Principle 4. Government as a platform- Agile Delivery and Reuse of Available Technology

The design, build and delivery of services is agile and we deliver value for money by reuse of components and assembling services more quickly. Reuse existing technologies in the architecture if they have the capability rather than introducing new technologies. Limit the number of suppliers to simplify supplier management and reduce overheads.

RATIONALE

Simply put, more technologies result in higher cost. Each discrete technology introduced into the architecture has a cost to it, this includes installation, licensing, maintenance, management, support and decommissioning.

IMPLICATIONS

Where possible, existing technology should be *reused* if it is "fit for purpose". If the existing technology is not fit for purpose, then it should be *replaced* with one that is across the IT estate. If no technology exists that meets a requirement, then a new technology can be *added* to the architecture however this should be infrequent and identified on the Technology Reference Model as a gap prior to progressing.

Principle 5. Interoperability

INTEROPERABILITY (USE OPEN / INDUSTRY STANDARDS)

Solutions should use Open and Industry Standards where possible to deliver solutions in alignment with GDS Technology Code of Practice.

RATIONALE

GDS maintains a list of Open Standards that are mandated for use and provides a mechanism for providing new standards to be included[5]. These, for the most part, are not relevant for BEIS DDaT operational systems but should be regularly reviewed[6]. The purpose of these Open Standards is to provide a level playing field for suppliers to compete on and to reduce lock-in to vendors. This principle has been expanded beyond the Open Standards requirement from GDS to include Industry Standards as leveraging standards that are used throughout the IT industry provides portability that cannot otherwise be achieved.

This model enables more competitive tenders to be completed resulting in lower cost and better outcomes.

The purpose of Open and Industry Standards is to provide interoperability and while "Industry Standards" are something that are defined, it should also be obvious what Industry Standards exist with a brief review of the market.

Some examples of industry standards are:

- RESTful JSON services for APIs
- SOAP over HTTPs for APIs (which is also referred to as ISO 40210)
- BPMN for Business Process Modelling (which is also referred to as ISO 19510)
- SQL for database querying (which is also referred to as ISO 9075)

Note, while several of the above examples are ISO standards, this is not a requirement for something to be considered an Industry Standard.

IMPLICATIONS

Any new systems added to the infrastructure should include

1. an analysis of the relevant standards used in industry
2. the standards that are supported by the shortlist of products

Systems which do not support the standards identified as mandatory should be marked down or excluded from the evaluation.

[5] https://standards.data.gov.uk/

[6] https://www.gov.uk/government/publications/open-standards-for-government

Principle 6. Security

The security of information, technology and services is essential to the maintenance of data confidentiality, service integrity and availability of information. All DDaT solutions should comply with the Cabinet Policy Security Policy Framework.[7]

RATIONALE

Getting security right has never been more important as the Civil Service continues to modernise and improve our ways of working, and deliver more and more services online. There are longstanding threats and risks to bear in mind; but we must also continue to develop our growing appreciation of global and cyber challenges, critical infrastructure dependencies, together with wider resilience and sustainability issues.

IMPLICATIONS

Architectural decisions involving primary storage of data should be carefully considered to ensure data is secure while being accessible.

Consistency of data should be considered with single source of truth being a principle of this. Data can also be stored in secondary locations for caching purposes but should be clearly described as secondary data.

[7] https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework#technology-and-services

Principle 7. Flexible and reliable solutions

The digital solutions that we implement can be improved or adapted quickly, in response to changing business or user needs.

Rationale

"Legacy systems" that are difficult to improve or adapt can inhibit change and will, in the long run, become expensive to maintain. In addition, integration of legacy systems with newer systems is usually complex and costly. As we move from legacy systems and hardware we will see the complexity of technology reduce and business areas will benefit from increased agility and efficiency.

Principle 8. TECHNOLOGY AND BUSINESS ALIGNMENT

Technology and Business Alignment

Investment in technology will be driven by business need to ensure maximum benefit for the organisation as a whole.

RATIONALE

IT provides a service to the wider organisation to support business operations. As such, the investment in technology should be made with consideration to the benefits to the business. Decisions should be driven based on overarching corporate strategy, and investment made to deliver on that strategy.

IMPLICATIONS

IT should be mindful that it is there to serve the "customer" – in this case the wider organisation. The organisation in turn services their customer (primarily those lodging and renewing IP rights).

This does not mean that non-IT departments should be making technology decisions, it means that the interests/requirements/needs of those departments should be considered when making technology decisions.

This also does not mean that IT should not invest in internal improvements and maintenance. There is a need to maintain systems including patching, monitoring, upgrading and consolidating. Where there is a significant investment, it should be justified – there is a separate principle on value for money.

Principle 9. COMPLIANCE AND LEGISLATION

All information managed within DDaT must comply with all relevant legislation, laws, policies and regulations and must be protected in how it is used and managed. This includes the GDS Technology Code of Practice[8] , Mandatory Requirements (MRs) set out in the Security Policy Framework.

RATIONALE

Compliance is mandatory in terms of information security. New regulations (e.g.: GDPR) and laws that come into force and might affect DDaT projects and services. All projects must be compliant with these laws, polices and regulations.

IMPLICATIONS

All information, both data and wider information, must be assigned Information Asset Owners who are responsible for the quality, integrity and suitability of the information.

Principle 10. Testing through continuous iteration

All changes/ projects/ solutions should be tested before being released out to users. Continuous testing should be carried out for each major output/feature of the software/ IT development.

RATIONALE

Without a well-thought testing phase, the project can fail and also impact the entire operational performance of the solution. With a poorly tested solution, the support and maintenance cost can escalate considerably and put in danger the reliability of the solution.

IMPLICATIONS

All projects planning should include testing phases for every development stage.

[8] https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice