Appendix H

Technical Design Authority Principles

Introduction

With an increasing number of ICT systems, suppliers and technologies, it is essential that technical principles are set and maintained to ensure the compatibility, integration and efficient operation across all services.

The Technical Architecture describes how all of the technical components fit and co-exist together. The Technical Design Authority is responsible for defining and maintaining DCC's Technical Architecture, and reporting proposed deviations from the standard architecture for further consideration by ITM.

The following are the set of Technical Principles set by DCC's Technical Design Authority. These principles must be used whenever purchasing a new ICT service or system. The Technical Design Authority must be advised whenever these principles cannot be met and they will assess the impact of and the cost of these exceptions.

These standards are designed to ensure Devon County Council moves towards ICT services that are:

- Cost effective
- Re-useable and flexible
- Integrated and collaborative
- Safe, secure and reliable
- Legal and compliant

Technical Principles

Information is Open

Where data has no Data Protection Act implications and is not sensitive in any other way, it will be made publically available.

Why?

Proactively sharing public data in an easy-to-access way will reduce the volume of FOI requests and improve the service to the public.

How?

We will publish open data in accordance with the latest guidance from GDS as found here: https://www.gov.uk/service-manual/technology/open-data.html

Systems are interoperable

The Government Digital Strategy open standards for software interoperability, data and document format enable software to interoperate through open protocols and allow the exchange of data between data stores and software through open data and document formats.

Why?

Utilising open standards for software interoperability, data and document formats in government IT specifications removes the potential for unintended barriers to digital participation.

How?

We will seek to adopt open standards agreed by GDS as published here: https://www.gov.uk/service-manual/making-software/open-standards-and-licensing.html

Data is Shared

People have access to the information they need to do to perform their duties. Data is shared, where appropriate, within the County Council and with partner organisations.

Why?

Appropriate automated sharing of data will enhance services and reduce resource required to respond to manual requests from partners.

Access to the right data leads to efficiency and effectiveness in decision-making. Staff time is saved and consistency of data is improved through one authoritative source of data.

How?

The system must have Application Program Interfaces compliant with open web interface standards, and be able to use these APIs to push and pull data to and from other systems as required using our Corporate Enterprise Service Bus (ESB).

Data must feed into the Corporate Data Warehouse for Business Intelligence purposes via the Corporate ESB.

Data is protected

Data will be protected and stored according to its business criticality and level of sensitivity.

Why?

DCC must meet the standards set out in the Data Protection Act to ensure that data is used fairly and lawfully, is not kept longer than is necessary, and is not unlawfully accessed or processed.

How?

Access, permissions and data protections are specified in accordance with the needs determined by the data owners regarding 'the need to know'. Examples of considerations are:

- The system must ensure access to the system is securely protected by allowing people to securely register an account.
- The system must enable users to securely create and re-set passwords.
- The system must only allow access to parts of the system the user should access (role based access).
- Web based systems with personally identifiable information or confidential data must be protected by two factor authentication.
- Data must be backed up at least nightly.
- Encryption appropriate to the sensitivity of the data must be used for both data in transit and data at rest.
- An ESCROW agreement must be in place for both the software "source code" and stored data of critical line of business systems.

Ease of use

Systems will be easy to use and require minimal training.

Why?

Systems that are intuitive to use will see faster and wider take-up with lower investment in training.

How?

New systems will be assessed by the intended user base before purchase to gauge how simple they are to use and how effectively they follow business processes.

Re-usable services

Wherever possible, applications and ICT services should be provided which can be used across the County Council. If an existing ICT solution meets the majority of the business requirements, and none of the missing requirements are critical or essential in nature, it should be used. If existing systems fail to meet critical business requirements, DCC will buy Commercial Off The Shelf Software (COTS) wherever possible. Building our own applications will always be the last resort.

Why?

The more ICT Services and systems there are, the higher the cost and complexity.

Where data is stored about the same person in multiple systems the risk of data being duplicated or conflicts occurring is higher.

How?

- Existing systems should be evaluated for suitability before buying new systems or ICT services.
- Where new services are required, consideration should be given to use within the wider Council.
- Devon must resist the need to customise applications to a Devon style - instead pursuing changes in organisation policies and principles to fit standard commercial offerings.

All browser based

Systems will be designed to work with current web standards (HTML5) and will be supported and fully functional on any currently supported version of common web browsers on Microsoft, Apple and Android-based client devices.

Why?

This is to ensure that systems can be accessed more widely and are not restricted to certain software being installed on specific devices. Additional costs are not incurred by needing to purchase, install and maintain additional technologies.

How?

- The system should not have any client device dependencies or software requirements beyond browser compatibility.
- Web access must support HTML5 and the presentation should be responsive to the type of device being used.

Software must be Accessible

All systems must meet standard accessibility standards.

Why?
DCC must ensure that people can access services and information, regardless of whether people have a disability or not.

How?
All web-based systems must meet current (W3C) Web Accessibility Standards
As a minimum, the system should meet Level AA of the Web Content Accessibility Guidelines (WCAG) 2.0.
Services should be tested for technical accessibility by an accessibility expert – W3C provides a range of Accessibility Evaluation Resources.

Systems must be Available

The system must be available for people to use when they need to use it.

Why?
The business cannot operate without the systems being available when they need them to be.

How?
The system must be resilient enough to remain available accordingly to the business criticality of the system, and in accordance with the respectively agreed SLA.

The system must be designed to have no single point of failure, and the Service Level Agreement must specify system availability KPIs commensurate with the service requirement.

This may include the adoption of failover technologies to ensure continued and uninterrupted availability of the system during the required hours of operation for highly critical business services.

Failure to meet an agreed level of system availability could result in penalties for the provider or service credits being issued.

Systems must use Common Identity Solutions

Systems must support the use of Common Identity Solutions which allow system users to log in using existing credential (user name and passwords).

Why?

Managing identity across multiple platforms is complex and costly. It can also be confusing for staff and citizens. We must endeavour to use the smallest number of different identity management solutions possible.

How?

For identity management of staff, the system should integrate with the corporate directory service, unless there is a very sound business requirement not to.

For partners, the system should federate with the credentials of their own organisation.

For citizen identity management, the system should integrate with the national identity management scheme, for example Verify.

Cloud First

When procuring new or replacement ICT services or systems, preference must always be given to Cloud Services first.

Why?
Supports Government 'Cloud First' policy for public sector IT

"Software as a Service", sometimes referred to as "hosted systems" normally operate on a subscription basis (ie you pay for what you use) and it is usually run (hosted) by the supplier.

Software as a Service allows flexibility for quickly increasing or decreasing numbers of people using the system.

Software as a Service means that systems are not locked into DCC's infrastructure and therefore if and when services are divested, they can be easily de-coupled from the County Council.

Supports the authority's vision of a smaller and agile workforce.

How?

- Software as a Service (SaaS) must be the first choice if an existing service cannot be re-used.
- Platform as a Service (PaaS) should be the second choice (an external supplier provides a technology to allow DCC ICT staff to develop and maintain systems on that platform)
- Infrastructure as a Service (IaaS) should be the third choice (this means that DCC ICT have to undertake all the work they would have done in-house but the infrastructure is hosted in the cloud)
- Where software is being provided as a service, the system should be client technology agnostic.
- The system should use standard internet connectivity (VPN and internet) and not require private lines.

Mobile by Design

Technology and systems will support people to work in a flexible way

Why?

The vision for DCC's future operating model is one of fewer staff being office-based workers, and more staff delivering services in a mobile and agile fashion. Systems and technology that require the use of traditional desktop and server hardware or wired network connections will be more costly and difficult to integrate in future, and will act as a brake on organisational transformation.

How?

The system must demonstrate flexibility with regard to hardware & software platforms and network connectivity.

Statutory and Legal Compliance

UK Legal standards and compliance for ICT services will be adhered to.

Why?

To ensure that DCC data is appropriately protected to demonstrate due diligence, and that in the event a serious

security incident does take place, we can demonstrate that all reasonable steps to achieve an acceptable level of risk.

How?

External suppliers must agree to adhere to relevant legal and regulatory requirements. These will include (but are not necessarily limited to) PSN IA, the NHS IG Toolkit and PCI-DSS.

External suppliers must agree to comply with industry recognised standards and DCC's approach to Open Data and Open Standards.

Services will comply with best practice guidelines by Central Government, for example, CESG Good Practice Guides and architectural patterns.

Secure by design

Data security must be considered at the earliest possible stage of a proposed project or application

Why?

It can be costly and create operational difficulties if security is an afterthought, bolted on after the design of a system is complete. The security needs of the data held in systems needs to be considered before any system design is finalised.

How?

CESG have published a design guide for creating secure services which will inform the design of all new services created by DCC; it can be found here: https://www.cesg.gov.uk/guidance/security-design-principles-digital-services-0 .

All business proposals for new systems must include the completion of the Privacy Impact Assessment document from Information Governance before any HLD is written or procurement commences so that a proper assessment of the inherent risks to data can be made.

High level design documents must consider the data security requirements and architecture of a proposed system.

For internet facing systems which hold personally identifiable or confidential data, the system is expected to have had an independent CHECK accredited penetration test within the last 12 months. Any identified vulnerabilities must have been acted

upon in accordance with the apparent risk, as assessed by the information asset owner and service provider.

Ongoing regular checks will be expected to be performed by suppliers on behalf of all their customers at least annually.

Where previous templates for the delivery of secure services exist they should be re-used where possible.

Delivered services will be validated against the original design to ensure there is no deviation that may affect security.

Mainstream Technology First

Commonly used technology and systems will be preferred. Lesser known technology or systems will not be used without full justification.

Why?

There are significantly increased costs for being "unique". It means that can be difficult to support systems as there are not a wide set of skills in the market place and it increases the cost of integrating with other systems.

How?

Maintain alignment to technical roadmap and target architecture.

Elasticity

Systems will be able to scale up and down in size and usage, providing flexibility to the County Council and its services as they change.

Why?

DCC is entering a period of substantial changes to service; deploying systems to meet a fixed requirement size will lead to inefficiencies and inflated costs if the underlying sizing requirements change.

How?

Systems that minimise overheads and are transparently and primarily costed on a per-use unit cost basis will be preferred over solutions with high overheads or complex charging structures.

Recoverable

The infrastructure must have appropriate plans for recovery of the technical components in the event of a disaster affecting the service.

Why?

All systems are vulnerable to failure, either due to issues with the system, the infrastructure it uses, or by external influence from unexpected sources. It is important that DCC services can continue in the face of unexpected events.

How?

The system must specify the approach to technical recovery in the event of a disaster and how normal service will be resumed. This must work hand in hand with Business Continuity Plans.

Must be commensurate with Recovery Time Objectives and Recovery Point Objectives as defined and agreed with the business.

Digital by Design

Services must deliver good quality, user centered, value for money digital services, websites and systems.

Why?

People expect to use digital services that are straightforward and convenient.

Digital Services mean people can engage with the Council when they want to, in a way they want to.

Digital Services reduce the need for manual intervention, improve the user experience and have lower overall service costs.

How?

Assessment of European Digital Capability Framework referenced within the Government Digital Strategy

Adherence to the LocalGov Digital Service Standard.