Luton

Technology Architecture Design Principles

April 2025

Author:	**Hazel Lunn**
Version:	**1.1 (draft)**
Date:	**17/03/2025**
Review Due:	**01/04/2026**

Contents

1. Purpose

This document establishes fundamental design rules to guide all architects and analysts in their work for Luton Council and partners. These rules are known as ‘architecture principles’ and will be applicable to anyone working in the Council who is acting as a change agent. Architecture principles are also used to guide selection of third-party products and services; in combination with functional and non-functional requirements for the specified change.

2. Introduction

This document presents a set of architecture principles for use at Luton Council. These principles apply to all individuals and to everything we do as a Local Authority. This version incorporates advances in cross-industry best practice (e.g. TOGAF v10); and it aligns with the developments in principles from our key stakeholder groups (e.g. the Government Digital Service and NHS Digital). It also supports our commitment as signatoriesof the local digital declaration.

Principles are general rules and guidelines that inform and support the way in which an organisation sets about fulfilling its mission. The application of architecture principles can bring many benefits to an organisation. Some of these benefits are:

• Design governance across IT and organisational change

• General rules and guidelines for the use and deployment of all IT resources and assets

• A basis for decision-making throughout an organisation which avoids inconsistency and favouritism

• A guide to relevant evaluation criteria and strategic influence on the selection of products and services

• Drivers for the definition of functional requirements for change

• Inputs to assess existing systems, the future strategic portfolio and insights into the transition activities needed to implement changes in support of business goals and priorities

A good set of principles should be:

1. **Understandable** - the intention of the principle is clear so that violations are minimized.

2. **Robust** - enable good quality decisions to be made, and enforceable policies and standards to be created.

3. **Complete** - every potentially important principle governing the management of information and technology for the organization is defined.

4. **Consistent** - principles should not be contradictory to the point where adhering to one principle would violate the spirit of another.

5. **Stable** - principles should be enduring, yet able to accommodate changes.

Principles may be established within different domains and at different levels. For example, it is common to have subsidiary principles within an organizational unit or in support of a major change programme. This document presents a complete set of solution principles, which are applicable to all designs, along with some associated overarching enterprise

principles. Dependent on the scope of the design being undertaken, additional principles may need to be considered. Any such additional principles must be able to coexist with the enterprise and solution principles. Principles in each of the solution domains (i.e. business, data, applications and technology) can be supplemented to address - or perhaps exploit - a given design constraint.

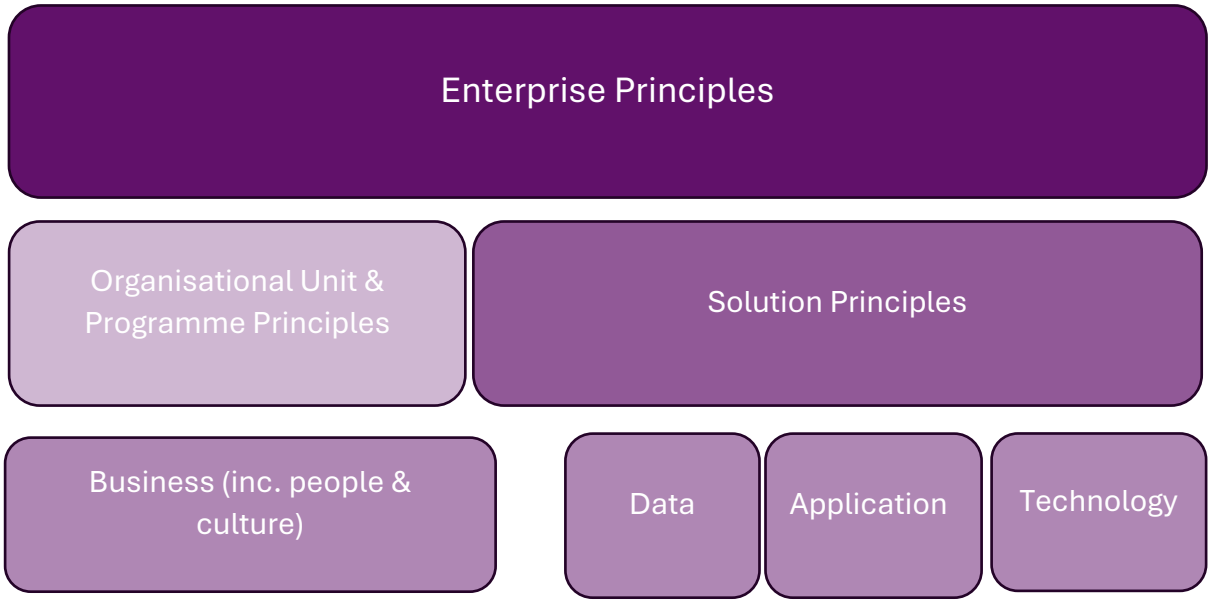

Diagram 1. Hierarchy of architecture design principles

The principles covered by this document span two levels as follows:

- **Enterprise Principles** providing the basis for harmonizing decision-making across the organisation, and informing how the organisation sets about fulfulling its mission. This includes Business and Data principles.
- **Solution Principles** embodying the spirit and thinking of the enterprise principles, and governing the architecture process. These include Application and Technology Principles.

All designs, incorporating business and technical change, should demonstrate adherance to all architecture principles. Exceptionally, however there may be justification for a waiver in adherence to an individual architecture principle for a proposed design if there is merit.

Luton Council will require all requests for new solutions and changes to existing solutions to go through an Architectural Design Authority (ADA) assessment process.

The Architectural Design Authority (ADA) ensures that all technology brought into the organisation is assessed for compatibility with the councils architecture. It is not a corporate decision making body, but the recommendation of the (ADA) must be taken into account by the body responsible for the introduction of the candidate technology. It is also the responsible body for monitoring the council's Enterprise Architecture, and ensures that all relevant documentation is effectively maintained.

Procurement approval will only be given by (ADA) if the council's infrastructure is not put at risk and solutions can only be supported by the Digital Data and Technology (DDaT) service if they have been approved by the (ADA).

The (ADA) process is attached in appendix 1 & 2.

3. Summary of Principles

The purpose of this section is to provide a list of the high-level principles that are defined in this document.

Pillar	Name	Statement
Business	**Primacy of Principles**	These principles apply to all departments within the enterprise.
	Compliance with Law	Enterprise information management processes comply with all relevant laws, policies, and regulations.
	Maximize Benefit to the Enterprise	Decisions are made to provide maximum benefit to the enterprise as a whole.
	Protection of Intellectual property	The enterprise's Intellectual Property (IP) must be protected. This protection must be reflected in the technology architecture, implementation, and governance processes.
	Information Management is Everybody's Business	All departments in the organisation participate in information management decisions needed to accomplish business objectives.
	Business Continuity	Enterprise operations are maintained despite system interruptions.
Data	**Data is an Asset**	Data is an asset that has value to the enterprise and is managed accordingly.
	Data is Shared	Users have access to the data necessary to perform their duties; therefore, data is shared across enterprise functions and organizations.
	Data is Accessible	Data is accessible for users to perform their functions.
	Data Security	Data is protected from unauthorized use and disclosure. In addition to the traditional aspects of national security classification, this includes, but is not limited to, protection of pre-decisional, sensitive, source selection-sensitive, and proprietary information.
Application	**Ease of Use**	Applications are easy to use. The underlying technology is transparent to users, so they can concentrate on tasks at hand.
	Technology Independence	Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms.
	Control Application Proliferation	The diversity and proliferation of applications is controlled to maximize return on investment and minimize the cost of maintaining expertise in multiple operational solutions and processes.
Technology	**Requirements Based Change**	Only in response to business needs are changes to applications and technology made.
	Responsive Change management.	Changes to the enterprise information environment are implemented in a timely manner.
	Control Technical Diversity	Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and

		connectivity between multiple processing environments
	Interoperability	Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.
	Microsoft First	Operating systems, software and relational database management systems should conform to Microsoft defined standards i.e., Microsoft Windows Server and Microsoft SQL Server etc.
	Agile, Innovative and Responsive	All technical solutions will support the organisational goal to embed agile and hybrid working for its staff.
	Digital by Design	The enterprise will use digital technologies to design and improve services, thinking more radically about how technology enablement can create simpler, cheaper and better services to customers.

4. Business Principles

E1. Primacy of Principles

Statement: These principles apply to all departments within the enterprise.

Rationale: The only way we can provide a consistent and measurable level of quality information to decision-makers is if all organizations abide by the principles.

Implications:

- Without this principle, exclusions, favouritism, and inconsistency would rapidly undermine the management of information and the validity of all of the principles.
- Inititives will not begin until they are examined for compliance with the principles.
- A conflict with a principle will be resolved by changing the framework of the initiative.

E2. Compliance with Law

Statement: Enterprise information management processes comply with all relevant laws, policies, and regulations.

Rationale: Enterprise policy is to abide by laws, policies, and regulations. This will not preclude business process improvements that lead to changes in policies and regulations.

Implications:

- The enterprise must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of data
- Changes in the law and changes in regulations may drive changes in our processes or applications. We must be prepared to implement compliance changes at pace and monitor risk of non compliance.

E3. Maximize Benefit to the Enterprise

Statement: Decisions are made to provide maximum benefit to the enterprise as a whole.

Rationale: This principle embodies "service above self". Decisions made from an enterprise-wide perspective have greater long-term value than decisions made from any particular organizational perspective. Maximum return on investment requires technology decisions to adhere to enterprise-wide drivers and priorities. No minority group will detract from the benefit of the whole. However, this principle will not preclude any minority group from getting its job done.

Implications:

- Achieving maximum enterprise-wide benefit will require changes in the way we plan and manage information — technology alone will not bring about this change
- Some teams may have to concede their own preferences for the greater benefit of the entire enterprise
- Application development priorities must be established by the entire enterprise for the entire enterprise
- Applications components should be shared across organizational boundaries
- As needs arise, priorities must be adjusted; a forum with comprehensive enterprise representation should make these decisions ie; Technology Steering Group.

E4. Protection of Intellectual Property

Statement: The enterprise's Intellectual Property (IP) must be protected. This protection must be reflected in the technology architecture, implementation, and governance processes.

Rationale: A major part of an enterprise's IP is hosted in the DDaT domain.

Implications:

- While protection of IP assets is everybody's business, much of the actual protection is implemented in the DDaT domain — even trust in non-tech processes can be managed by DDaT processes (email, notes, etc.).
- A policy, governing human and IT actors, will be required that can substantially improve protection of IP; this must be capable of both avoiding compromises and reducing liabilities.

E5. Information Management is Everybody's Business

Statement: All departments in the organisation participate in information management decisions needed to accomplish business objectives.

Rationale: Information users are the key stakeholders, in the application of technology to address a business need. To ensure information management is aligned with the business, all departments in the organsiation must be involved in all aspects of the information environment. The business experts from across the organisation and the technical staff responsible for developing and sustaining the information environment need to come together as a team to jointly define the goals and objectives of Technology.

Implications:

- To operate as a team, every stakeholder, will need to accept responsibility for developing the information environment.
- Commitment of resources will be required to implement this principle.
- Clear data ownship needs to be at the heart of the organisation.

E6. Business Continuity

Statement: Enterprise operations are maintained despite system interruptions

Rationale: As system operations become more pervasive, we become more dependent on them; therefore, we must consider the reliability of such systems throughout their design and use. Business premises throughout the organisation must be provided with the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop enterprise activities. The enterprise business functions must be capable of operating on alternative delivery mechanisms.

Implications:

- Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed. This includes but is not limited to periodic reviews, testing for vulnerability and exposure, or designing mission-critical services to ensure business function continuity through redundant or alternative capabilities.
- Recoverability, redundancy, and maintainability should be addressed at the time of design.
- Applications must be assessed for criticality and impact on the organisations priorities, in order to determine what level of continuity is required and what corresponding recovery plan is necessary.

5. Data Principles

E7. Data is an Asset

Statement: Data is an asset that has value to the enterprise and is managed accordingly

Rationale: Data is a valuable corporate resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most corporate assets are carefully managed, and data is no exception. Data is the foundation of our decision making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.

Implications:

- There is an education task to ensure that users in the organisation understand the relationship between value of data, sharing of data, and accessibility to data.
- Data stewardss must have the authority and means to manage the data for which they are accountable.

- We must make the cultural transition from "data ownership" thinking to "data stewardship" thinking.
- The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to enterprise personnel and adversely affect decisions across the enterprise.
- Part of the role of data steward, who manages the data, is to ensure data quality procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed information. Data quality will need to be measured and steps taken to improve data quality — it is probable that policy and procedures will need to be developed for this as well.
- A forum with comprehensive representation should decide on process changes ie; Data Governence board.
- Since data is an asset of value to the entire enterprise, data stewards accountable for properly managing data must be of the appropriate seniority.

E8. Data is Shared

Statement: Users have access to the data necessary to perform their duties; therefore, data is shared across enterprise functions and organizations.

Rationale: Timely access to accurate data is essential to improving the quality and efficiency of enterprise decision-making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The enterprise holds a wealth of data, but it is stored in seperate databases. Shared data will result in improved decisions since we will rely on fewer (ultimately one virtual) sources of more accurate and timely managed data for all of our decision-making.

Implications:

- There is an education task to ensure that all departments understand the relationship between value of data, sharing of data, and accessibility to data.
- To enable data sharing we must develop and abide by a common set of policies, procedures, and standards governing data management and access for both the short and the long term
- For the short term, to preserve our significant investment in legacy systems, we must invest in software capable of migrating legacy system data into a shared data environment
- We will also need to develop standard data models, data elements, and other metadata that defines this shared environment and develop a repository system for storing this metadata to make it accessible
- For the long term, as legacy systems are replaced, we must adopt and enforce common data access policies and guidelines for new application developers to ensure that data in new applications remains available to the shared environment and that data in the shared environment can continue to be used by the new applications
- For both the short term and the long term we must adopt common methods and tools for creating, maintaining, and accessing the data shared across the organisation.
- This principle of data sharing will continually conflict the principle of data security — under no circumstances will the data sharing principle cause confidential data to be compromised.

- This will ensure that only the most accurate and timely data is relied upon for decision-making. Shared data will become the enterprise-wide "virtual single source" of data.
- Investment in skills and resources are required to move to an enterprise-wide data source.

E9. Data is Accessible

Statement: Data is accessible for users to perform their functions.

Rationale: Wide access to data leads to efficiency and effectiveness in decision-making, and affords a timely response to information requests and service delivery. Using information must be considered from an enterprise perspective to allow access by a wide variety of users. Staff time is saved, and consistency of data is improved.

Implications:

- There is an education task to ensure that all departments within the organisation understand the relationship between value of data, sharing of data, and accessibility to data.
- Accessibility involves the ease with which users obtain information
- The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of users and their methods of access
- Access to data does not constitute understanding of the data — Users should take caution not to misinterpret information
- Access to data does not necessarily grant the user access rights to modify or disclose the data This will require an education process and a change in the organizational culture, which currently supports a belief in "ownership" of data by functional units.

E10. Data Security

Statement: Data is protected from unauthorized use and disclosure. In addition to the traditional aspects of national security classification, this includes, but is not limited to, protection of pre-decisional, sensitive, source selection-sensitive, and proprietary information.

Rationale: Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information. Existing laws and regulations require the safeguarding of personal and sensitive data, while permitting free and open access. Pre-decisional (work-in-progress, not yet authorized for release) information must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use.

Implications:

- Aggregation of data, both classified and not, will create a large target requiring review and de-classification procedures to maintain appropriate control Data owners and/or functional users must determine whether the aggregation results in an increased classification level. Appropriate policy and procedures will be needed to handle this review and declassification. Access to information based on a need-to-know policy will force regular reviews of the body of information.

- To adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level
- Data security safeguards can be put in place to restrict access to "view only" or "never see" Sensitivity labelling. However data labelling standards need to be adopted by all.
- Security must be designed into data elements from the beginning; it cannot be added later systems, data, and technologies must be protected from unauthorized access and manipulation. Data must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure.

6. Application Principles

S1. Ease of Use

Statement: Applications are easy to use for staff and residents where it is a public facing system. The underlying technology is transparent to users, so they can concentrate on tasks at hand.

Rationale: The more a user has to understand the underlying technology, the less productive that user is. Ease-of-use is a positive incentive for use of applications. It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish the task outside of the enterprise's integrated information environment. Most of the knowledge required to operate one system will be similar to others. Training is kept to a minimum, and the risk of using a system improperly is low. Using an application should be intuitive.

Implications:

- Applications will be required to have a common "look-and-feel" and support ergonomic requirements; hence, the common look-and-feel standard must be designed and usability test criteria must be developed.
- Factors such as linguistics, physical infirmities (visual acuity, ability to use keyboard/mouse), and proficiency in the use of technology have broad ramifications in determining the ease-of-use of an application.
- Application interfaces must meet accessibility standards.
- Workflows must be designed with user centric design.
- Applications should be configured not customised. This may conflict with Business need if the application is not fit for purpose in the first place.

S2. Technology Independence

Statement: Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms.

Rationale: Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost effective and timely way. Otherwise, technology, which is subject to continual obsolescence and vendor dependence, becomes the driver rather than the user requirements themselves. The intent of this principle is to ensure

that Application Software is not dependent on specific hardware and operating systems software.

Implications:

- This principle will require standards which support portability.
- For Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) applications, there may be limited current choices, as many of these applications are technology and platform dependent.
- Subsystem interfaces will need to be developed to enable legacy applications to interoperate with applications and operating environments developed under the Enterprise Architecture.
- Middleware should be used to decouple applications from specific software solutions and act as an interface between solutions.
- As an example, we will avoid oracle only based applications as we have limited oracle based capacity and skills.

S3. Control Application Proliferation

Statement: The diversity and proliferation of applications is controlled to maximize return on investment and minimize the cost of maintaining expertise in multiple operational solutions and processes

Rationale: This principle embodies the terms of "shadow IT" because many of these applications are brought into the organization by business users rather than the DDaT service. This practice will create issues for the enterprise and the technology department as applications are often acquired for user-centric purposes, rather than for attaining the overall mission of the enterprise.

Application proliferation will require centralized control. We have application assets dispersed throughout various platforms:

- In the cloud.
- In co-location data centres.
- On premises.
- In various SaaS environments.

The enterprise requires a single pane of glass that gives them insight into their entire application portfolio. When they have that kind of control, the principal risks of identity sprawl, data dissipation, and the enlargement of the threat surface will be much easier to manage. Therefore, reducing and rationalising the number of applications across the organisation will make it easier and cheaper to manage the digital infrastructure.

Implications:

- Having many applications at once engenders identity sprawl. This forces users into bad password practices—reusing passwords, for example, or not changing them regularly—which then puts the organization at risk. We therefore deploy single sign on (SSO) as preferred method across the portfolio. Multi-factor authentication (MFA) is also critical to guard against a cybercriminal obtaining an employee's credentials in a username-password access system.

- Application proliferation will increase the risk of data dissemination and dissipation across multiple applications, different versions of the same data can end up stored in multiple places, and multiple copies means multiple versions of what should be one truth exist, potentially creating confusion. To combat the enterprise should publish guidelines for business-led teams to educate them on data hygiene and the health of data in applications.
- Application proliferation will increase the size of the enterprise “threat surface”, which is a significant security risk. With every added layer of complexity, there are more vulnerabilities, and more risk to manage. To fight against these risks and vulnerabilities the enterprise should not only secure its network, but also focus on application security by using web application firewalls. The more applications in use the larger the security portfolio becomes too.
- Application development, purchase and implementation priorities must be established by the entire enterprise for the entire enterprise.
- Applications components should be shared across organizational boundaries.
- As needs arise, priorities must be adjusted; The Architectural Design Authority, should make decisions around the development, procurement, and implementation of applications to control the expansion in enterprise application portfolios.

7. Technology Principles

S4. Requirements Based Change

Statement: Only in response to business needs are changes to applications and technology made.

Rationale: This principle will foster an atmosphere where the technology environment changes in response to the needs of the business, rather than having the business change in response to technology changes. This is to ensure that the purpose of the technology supports the transaction of business. Unintended effects on business due to Technology changes will be minimized. A change in technology may provide an opportunity to improve the business process and, hence, change business needs.

Implications:

- Changes in Technology will follow full examination of the proposed changes using the Architetural Design Authority.
- There is no funding for a technical improvement or system development unless a documented business need exists. This may require business processes documenting and a business case for change.
- Change management processes conforming to this principle will be developed and implemented.
- This principle may conflict against the responsive change principle. We must ensure the requirements documentation process does not hinder responsive change to meet legitimate business needs. The purpose of this principle is to keep the focus on business, not technology needs — responsive change is also a business need.
- Application roadmaps and development plans must be agreed with the business.
- The underlying infrastructure must be considered as part of any change. We have a hybrid environment and so can operate, Saas, on prem or Azure based applications.

The underlying cost of operating needs to be considered to determine the most cost effective environment for the solution to be based in.

S5. Responsive Change Management

Statement: Changes to the enterprise technology environment are implemented in a timely manner.

Rationale: If people are to be expected to work within the enterprise technology environment, that environment must be responsive to their needs.

Implications:

- Processes for managing and implementing change must not create delays.
- The Change Approval process must include input from a "business expert" to facilitate explanation and implementation of that need.
- If changes are going to be made, the architectures must be kept updated
- This will conflict with other principles (e.g., maximum enterprise-wide benefit, enterprise-wide applications, etc.)

S6. Control Technical Diversity

Statement: Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments

Rationale: There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained. Limiting the number of supported components will simplify maintainability and reduce costs. The business advantages of minimum technical diversity include:

- standard packaging of components.
- predictable implementation impact.
- predictable valuations and returns.
- redefined testing.
- utility status, and
- increased flexibility to accommodate technological advancements.

Common technology across the enterprise brings the benefits of economies of scale to the enterprise. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

Implications:

- Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle
- Technology choices will be constrained by the choices available within the technology blueprint.

- The technology baseline is not being frozen Technology advances are welcomed and will change the technology blueprint when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated.
- We have a flexible enough infrastructure to allow for most scenarios but control is there to standardise and reduce cost.

S7. Interoperability

Statement: Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.

Rationale: Standards help ensure consistency, thus improving the ability to manage systems, improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products and facilitate supply chain integration.

Implications:

- Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a nonstandard solution
- The process for setting standards, reviewing, and revising them periodically, and granting exceptions is the Architectural Design Authority review.
- The existing Technology platforms must be identified and documented.

S8. Microsoft First

Statement: Operating systems software and relational database management systems should conform to Microsoft defined standards i.e., Microsoft Windows Server and Microsoft SQL Server etc.

Rationale: Using a Microsoft technology will ensure a consistency across the architecture, improve the ability of the DDaT service to manage systems, increase security and help to reduce costs.

Implications:

- Microsoft standards for operating systems and relational database management systems will be utilised unless there is a compelling reason to implement a nonstandard solution.
- If Microsoft solutions are already implemented across the enterprise, their built-in functionality and services should be reviewed as part of a requirements management process prior to the procurement and implementation of another vendor solution.
- A Microsoft-centric architecture will help an organisation maximise its return on investment of software licencing from this vendor, by utilising the greatest number of services provided by enterprise-level applications such as Microsoft Office 365.
- An investment in skills is required to fully maximise the use of products on offer as part of enterprise licensing and increase our development capabilities.
- Any migration plan away from other solutions to a microsoft product must adhere to the other priciples.

S9. Agile, Innovative and Responsive

Statement: All technical solutions will support the organisational goal to embed agile and hybrid working for its staff.

Rationale: Regardless of whether staff are sitting at a desk in a council office, using a laptop while working from home, or on a smartphone while working in the field, all enterprise systems and applications should work, so they can concentrate on delivering against their designated role.

Implications:

- Mobile applications will be responsive and effortless to use, to ensure that staff can complete their tasks efficiently.
- Designing access to networks and applications will require complex security controls. It is essential that user are not hindred or have visability of these controls. With the expection of MFA.
- As so many users now rely on technology to do their jobs, response to incidents and servicedeks requests must keep pace with expectation.
- The business continuity plans need to take into account loss of systems, restoration of services and the needs of the users from a communication and continuity of business perspectve.

S10. Digital by Design

Statement: The enterprise will use digital technologies to design and improve services, thinking more radically about how technology enablement can create simpler, cheaper and better services to customers.

Rationale: Using modern technology and automation will reduce duplication of effort, allocate work more quickly and without paperwork and bureaucracy, enabling the enterprise to deliver faster services whilst improving customer satisfaction

Implications:

- Digital solutions will aspire to be intuitive, straightforward and require minimal user training.
- Users will be consulted when designing solutions to ensure that the finished product meets their needs and the needs of the business.
- All processes and services will be examined from start to finish to determine how they can be simplified, the duplication of data can be prevented, and customer-centricity built in. This requires investment in resources.
- Investment in flexible, generic and low code platform technologies that will offer the enterprise core functionality to enable it to digitise processes and redesign services efficiently.
- The enterprise will share information and simplify procedures and services to provide better outcomes for its customers and partners.