ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

Architecture Principles

Author:	Craig Douglas
Date:	30 October 2014

Document Security Level:	**PUBLIC**
Document Version:	2.0
Document Ref:	<IT document reference code if applicable>
Document Link:	<URL>
Review Date:	October 2015

Architecture Principles

Table of Contents

Architecture Principles

Introduction

Enterprise Architecture Principles are high level statements of the fundamental values that guide Business Information Management, Information Technology (IT) decision-making and activities, and are the foundation for both business and IT architectures, standards, and policy development.

These principles are general rules and guidelines that may be subject to adjustments as the enterprise refocuses its objectives and mission. However, they are intended to be enduring and not prone to frequent amendments.

They inform and support the way in which and Plymouth University sets about fulfilling its mission.

Principles are established on all Enterprise Architecture Domains:

Business - provide a basis for decision-making throughout the business

Data - provide guidance of data use within the enterprise

Application - provide guidance on the use and deployment of all IT applications

Technology - provide guidance on the use and deployment of all IT technologies

Decisions and business cases are strengthened by compliance with these principles. Where there are conflicts of interest between, for example, two solution development projects, then these principles should guide the decision making. If proposed changes do not comply with these principles then the changes should be realigned with the principles.

Figure 1 below, shows the level of detail provided by each element of the governance structure on the IT lifecycle and indicates that the architectural principles which follow have a fairly major influence on how IT implementations are designed, developed and run within Plymouth University going forward. It can be seen that these principles should not be used independently of other guiding documents such as technology

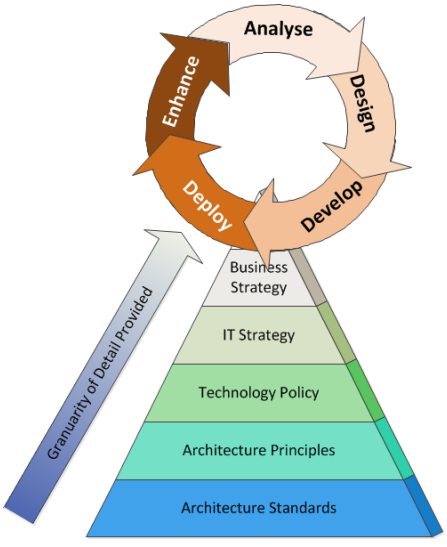

Figure 1: Level of Detail Provided to Implementation

Figure 2: Effect of Governance on Implementation

policy documents and architectural standards and must be aligned with IT and business strategy.

Figure 2 above, shows how these architectural principles and the other operational governance documents influence all stages of the IT lifecycle and should be aligned with to ensure the benefits of an architectural approach to system and service design are realised as real benefits to the University.

Architecture Principles

Business Principles

Principle 1: Primacy of Principles

Statement:	These architectural principles will apply to all organisational units within the enterprise.
Rationale:	The only way the University will be able to provide a consistent and measurable level of appropriately robust, reliable, sustainable services and quality information to decision-makers, is if all stakeholders abide by the University's overarching principles for its technology, information and business architectures.
Implications:	• This fundamental principle will ensure inclusion, consistency, fairness and continual alignment to the business. Without this the management of our technologies, information and business processes would be quickly undermined. • Business Partners engaging with the business will work to find accommodation between interested parties around any conflicts with a principle relevant to the proposal.

Principle 2: Compliance with Statutory Obligations

Statement:	Enterprise data and information management processes comply with all relevant internal and external 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 all laws, regulations, and external policies regarding the collection, retention, and management of data. • Continual education, access and awareness to the rules must be maintained. • Efficiency, need, and common sense are not the only drivers. Changes in the law and changes in regulations may drive changes in our processes or applications.

Principle 3: Maximise Benefit to the Enterprise

Statement:	Information management decisions are made to provide maximum benefit to the enterprise as a whole within the Plymouth University governance frameworks.
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 organisational perspective. Maximum return on investment requires information management decisions to adhere to enterprise-wide drivers and priorities. No Organisation Unit will detract from the benefit of the whole. However, this principle will not preclude any Organisation Unit 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 organisations 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 organisational boundaries. • Information management initiatives should be conducted in accordance with the enterprise plan. Individual organisations should pursue information management initiatives which conform to the blueprints and priorities established by the

	enterprise. We will change the plan as we need to. • As needs arise, priorities must be adjusted. The Enterprise Architecture Board will make these decisions.

Principle 4: Information Management is Everybody's Business

Statement:	All organisations in the enterprise participate in information management decisions needed to accomplish business objectives.
Rationale:	Information users are the key stakeholders, or customers, in the application of technology to address a business need. In order to ensure information management is aligned with the business, all organisations in the enterprise must be involved in all aspects of the information environment. The business experts from across the enterprise 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 IT.
Implications:	• To operate as a team, every stakeholder, or customer, will need to accept responsibility for developing the information environment. • Commitment of resources will be required to implement this principle.

Principle 5: Business Continuity

Statement:	Enterprise operations are maintained regardless of any system interruptions.
Rationale:	As system operations become increasingly pervasive, we become more dependent on them; therefore, we must consider the reliability of such systems throughout their design and use. Where possible, critical business functions throughout the enterprise must be provided with the capability to continue regardless of external events, such as but not limited to; hardware failure, natural disasters or data corruption. The enterprise business functions must be capable of operating on alternative information delivery mechanisms, we will look to enhance this capability over time.
Implications:	• Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed. • Management 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 enterprise mission in order to determine what level of continuity is required and what corresponding recovery plan is necessary. • Metrics surrounding availability, operational and service level agreements must be mandated as part of the design process.

Principle 6: Common Use Applications

Statement:	Solutions that can be applied across the enterprise are preferred to the development of solutions which are only provided to a particular organisation unit.
Rationale:	Duplicative capability is expensive and can result in the proliferation of conflicting data.

Implications:	• Organisation units which depend on a capability which does not serve the entire enterprise must change over to the replacement enterprise-wide capability. This will require establishment of and adherence to a policy requiring this. • Organisation units will not be allowed to develop capabilities for their own use which duplicate enterprise-wide capabilities. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced. • Data and information used to support enterprise decision-making will be standardised. This is because the smaller, organisational capabilities which produced different data (which was not shared among other organisation units) will be replaced by enterprise-wide capabilities. The impetus for adding to the set of enterprise-wide capabilities may well come from an organisation unit making a convincing case for the value of the data/information previously produced by its organisational capability, but the resulting capability will become part of the enterprise-wide system, and the data it produces will be shared across the enterprise. • Ambiguities resulting from multiple insular definitions of data must give way to accepted enterprise-wide definitions and understanding. • Multiple data standardisation initiatives need to be coordinated. • Functional data administration responsibilities must be assigned. • Where appropriate an enterprise single sign-on should be utilised alongside role based access control to maintain data security.

Principle 7: IT Responsibility

Statement:	The IT organisation is responsible and accountable for owning and implementing all IT processes and infrastructure that enable solutions to meet business-defined requirements for functionality, service levels, cost, and delivery timing. Decisions should always align back to the requirement of the Business.
Rationale:	Effectively align expectations with business requirements and our overall capabilities so that all projects are cost-effective and can be completed in a timely manner. Efficient and effective solutions should have reasonable costs and clear benefits relative to the business proposition.
Implications:	• The IT function must define processes to manage business expectations and priorities. • Projects must follow an established process to reduce costs and to ensure the project has a timely completion • Data, information, and technology should be integrated to provide quality solutions and to maximise results.

Principle 8: Data Security

Statement:	All data that is classified as being confidential, sensitive or personal will be protected from unauthorised use and disclosure; 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 security and the privacy of data, while permitting free and open access. Pre-decisional (work-in-progress, not yet authorised 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 declassification procedures to maintain appropriate control. Data stewards and/or functional users must determine whether the aggregation results in an increased classification level. We will need appropriate policies and procedures 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. • Processes will need to address the classification of data being dealt with and when or if it is suitable to declassify for wider consumption. • In order 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 for access to pre-decisional, decisional, classified, sensitive, or proprietary information must be determined. • Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorised access and manipulation. Vice Chancellor’s Executive information must be safeguarded against inadvertent or unauthorised alteration, sabotage, disaster, or disclosure. • Need new policies on managing duration of protection for pre-decisional information and other works-in-progress, in consideration of content freshness.

Principle 9: 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, in doing so data assets can provide additional value to academic and research endeavours.
Implications:	• This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organisations within the enterprise understand the

	relationship between value of data, sharing of data, and accessibility to data. • We must make the cultural transition from ‘‘data ownership’’ thinking to ‘‘data stewardship’’ thinking. • Since data is an asset of value to the entire enterprise, data stewards accountable for properly managing the data must be assigned at the enterprise level. • Stewards must have the authority and means to manage the data for which they are accountable. • The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to personnel and adversely affect decisions across the enterprise. • Part of the role of data steward 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.

Principle 10: Data is Shared

Statement:	Users have access to the data necessary to perform their duties; therefore, data is shared across enterprise functions and organisations.
Rationale:	Maintaining data in a single environment (“single source of truth”) and then sharing it in response to business needs has distinct advantages for the organisation: Speeds data collection, creation, transfer, and assimilation. Improves the quality and efficiency of enterprise decision-making which will be based on timely and accurate data. It reduces the costs associated with data management by eliminating the need to maintain multiple databases. Electronically shared data will also result in increased efficiency when existing data entities can be used, without re-keying, to create new entities.
Implications:	• This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organisations within the enterprise 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, discovery and access for both the short and the long term. • Data should be defined consistently throughout the enterprise, using definitions that are understandable and available to all users. This can be achieved by developing and maintaining an enterprise data dictionary. • 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 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. • 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 enterprise. • Data sharing will require a significant cultural change. • This principle of data sharing will continually conflict with the principle of data security. Under no circumstances will the data sharing principle cause confidential, personal or sensitive data to be compromised. • Data made available for sharing will have to be relied upon by all users to execute their respective tasks. 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. • Data where applicable, will be available externally to the enterprise. This will afford both rich service provision and also the ability to perform research collaboratively with partners.

Principle 11: 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 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:	• This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organisations within the enterprise 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 enterprise users and their corresponding methods of access. • Access to data does not constitute understanding of the data. Personnel 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 organisational culture, which currently supports a belief in ''ownership'' of data by functional units.

Principle 12: Data Trustee

Statement:	Each data element has a trustee accountable for data quality.
Rationale:	One of the benefits of an architected environment is the ability to share data (e.g., text, video, sound, etc.) across the enterprise. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the data trustee makes decisions about the content of data. Since data can lose its integrity when it is entered multiple times, the data trustee will have sole responsibility for data entry which eliminates redundant human effort and data storage resources. Note: A trustee is different than a steward — a trustee is responsible for accuracy and currency of the data, while responsibilities of a steward may be broader and include data standardisation and definition tasks.
Implications:	• Real trusteeship dissolves the data ''ownership'' issues and allows the data to be available to meet all users' needs. This implies that a cultural change from data

	‘‘ownership’’ to data ‘‘trusteeship’’ may be required. • The data trustee will be responsible for meeting quality requirements levied upon the data for which the trustee is accountable. • It is essential that the trustee has the ability to provide user confidence in the data based upon attributes such as ‘‘data source’’. • It is essential to identify the true source of the data in order that the data authority can be assigned this trustee responsibility. This does not mean that classified sources will be revealed nor does it mean the source will be the trustee. • Information should be captured electronically once and immediately validated as close to the source as possible. Quality control measures must be implemented to ensure the integrity of the data. • As a result of sharing data across the enterprise, the trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and, subsequently, must then recognise the importance of this trusteeship responsibility.

Principle 17: Data will be Analysable

Statement:	Data assets provide invaluable information to the enterprise for research and business intelligence decision-making when gathered, stored and accessed correctly.
Rationale:	Making sound business decisions at all levels across the university is aided significantly by having access to timely accurate data from all systems, presented in the most appropriate way for the consumer. Holding this data for all systems, services, functions and processes will enable an enterprise wide view on our estate, capabilities and the best utilisation of our resources throughout. Systems included go beyond our traditional monitoring points of student, staff and financial data and will include areas such as, but not limited to, physical space usage, telephony usage, email usage, network statistics, all other areas of IT and beyond.
Implications:	• Data will be gathered from *all* capable systems and stored in a centralised data warehouse repository. • Data which includes elements, which may be classified as personally identifiable, will be anonymised prior to being committed to the repository. • All new systems will be procured with the capability to store logs and other pertinent information within the repository. • In order to ensure a sound basis for analysis, existing systems will be examined to ensure they are able to supply relevant data to the repository. • Suitable analytical software will be used to extract required data from the repository and present to the consumer in the most appropriate way. • This data and the subsequent use of it will be subject to Information Security and Information Management policies, procedures and classifications as set out by Plymouth University. • “Data will meet data quality standards of accuracy, validity, reliability, timeliness, relevance, completeness and compliance with University regulations and statutory obligations, as established by the Data Quality Policy (draft).”

Principle 13: Technology Independence

Statement:	Services delivered as part of the university provision are independent of specific technology choices and therefore can operate on a variety of technology platforms. Applications should, as much as possible, be independent in terms of the technology they are consumed on.
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. Realising that every decision made with respect to IT makes us dependent on that technology, the intent of this principle is to ensure that application software is not dependent on specific hardware and operating systems software. Exit strategies should be implemented when considering a technology, facilitating an agnostic approach that may change if the service needs change.
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 hese 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.

Principle 14: Ease of Use

Statement:	Applications are easy to use. 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.
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 and take into account the importance of "transferrable skills" whilst working with any given product. • Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability. Factors such as linguistics, customer 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. • Concentration should be to deliver ease at the point of consumption. There is recognition that to provide this expertise must be developed or bought.

	• Digital literacy will impact on determining the balance between expected levels of competence and ease-of-use.

Principle 18: Purchase rather than Develop

Statement:	Component technology, application and services shall, as much as possible, be purchased off the shelf.
Rationale:	Commercial products provide a greater longevity, supportability and are therefore more sustainable; whereas in house developments are likely to be constrained by the developer of the solution and their availability. Acquiring commercial products provide a greater level of support, knowledge and upgradeability than can be afforded by internal developments. Any new products procured for the enterprise, must be able to integrate with the existing architecture, unless it is replacing or significantly enhancing the current provision of service. Otherwise software diversity increases and reduces the effectiveness of our ability to serve the needs of our customers. Commercial Off-The-Shelf (COTS) products often provide a wealth of business logic, process modelling and workflows already developed or that can been altered to meet the enterprises requirements. Roadmaps detail forthcoming improvements, in terms of security and functionality which ultimately benefit the planning processes; these business essentials are not present in solutions that are locally engineered.
Implications:	• This principle will require standards which support sustainability. • Formalised training programmes can be undertaken for both developers and staff managing the solution, thus enhancing both staff knowledge and expediting the benefits afforded to the business. • Following the initial set-up of the product, integration with additional systems should facilitate agile development.

Principle 15: 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 information environment changes, in a timely and controlled manner, in response to the needs of the business, rather than having the business change in response to IT changes. This is to ensure that the purpose of the information support — the transaction of business — is the basis for any proposed change. Unintended effects on business due to IT changes will be minimised. A change in technology may provide an opportunity to improve the business process and, hence, change business needs.
Implications:	• Changes in implementation will follow full examination of the proposed changes using the enterprise architecture. • We will not fund a technical improvement or system development unless a documented business need exists. • Change management processes conforming to this principle will be developed and implemented. • Agreed changes will be implemented in a timely manner. • 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 us focused on business, not technology needs — responsive change is also a business need.

Principle 16: Control Technical Diversity

Statement:	Technological diversity is controlled to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments. We accept that there is never a one size fits all model, but endeavour that technology components are able to work together. However, determent to the end users' experience should be limited.
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. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and put in place. • We are not freezing our technology baseline. We welcome technology advances and will change the technology blueprint when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has

	been demonstrated.

Glossary of Terms

Architecture principles	A qualitative statement of intent that should be met by the architecture. Has at least a supporting rationale and a measure of importance.
Capability	A business-focused outcome that is delivered by the completion of one or more work packages. Using a capability-based planning approach, change activities can be sequenced and grouped into order to provide continuous and incremental business value.
Data steward	Data stewards are senior officials or their designees with management responsibility for defined segments of enterprise data, and planning/policy making responsibility for data within their functional areas. Working at the enterprise level, they will contribute to data standardisation and definition to ensure data quality and enable data sharing across the organisation.
Data trustee	Data trustees have direct operational-level responsibility for the management of a subset of data, ensuring data quality in terms of accuracy, currency and integrity.
Enterprise	The highest level (typically) of description of an organisation and typically covers all missions and functions. An enterprise will often span multiple organisations.
Organisational unit	A self-contained unit of resources with line management responsibility, goals, objectives and measures.

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.1	Craig Douglas	Enterprise Architect	Initial Document	04/02/2014	<Print name>	<Job Title>	<dd/mm/yyyy> <hh:mm>
0.2	Craig Douglas	Enterprise Architect	Amended following EAB	14/02/2014			
0.3	Craig Douglas	Enterprise Architect	Amended following TIS SLT	28/03/2014			
1.0	Craig Douglas	Enterprise Architect	Corrected & Approved Following CIO feedback	07/04/2014	John Wright	CIO	April 2014
1.1	Craig Douglas	Enterprise Architect	Principles 17 & 18 Added	24/09/2014	Enterprise Architecture Board		22/09/2014
2.0	Craig Douglas	Enterprise Architect	Updated to New Template	30/10/2014	Paul Westmore	IT Director	23/10/2014