ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-010-Architecture Service Planning Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	24/06/2015
Document Security Level:	**PUBLIC**
Document Version:	1.00
Document Ref:	EA-ISP-010
Document Link:	<URL>
Review Date:	June 2016

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	PF	ESA	Initial draft	12/02/2014			
0.91	SF, PD	Head of School of Computing, Associate Professor	Comments on draft	04/03/2014			
0.92	PF	ESA	Updated with new document format, added greater details around section 4 and added section 5	13/02/2015			
0.93	PF	ESA	Altered section 1 to ensure consistency with authorisation channels	19/03/2015			
0.94	PF, CD	ESA, EA	Inclusion of System Lifecycle information	24/03/2015			
0.95	PF, CD	ESA, EA	Alteration of document to refocus on services in place of solely systems	18/06/2015 11:00			
0.96	PF, LF	ESA, AIS	Slight tweak for Acceptance into Service section	24/06/2015			
1.00	PF, CD, PW, DM	ESA, EA, IT Director, Operations Manager	Alteration to Architecture Service Planning Policy	26/06/2015 15:20	Paul Westmore	IT Director	26/06/2015 13:30

EA-ISP-010-Architecture Service Planning Policy

Introduction

This policy forms part of the University's Information Security Policy Set and should be read in conjunction with the Information Security Policy (EA-ISP-001), Data Classification Policy (EIM-POL-001), Software Management Policy (EA-ISP-013) and Information Handling Policy (EA-ISP-007).

The Service Planning Policy sets out how information services or systems are specified, designed and include processes for identifying requirements and risks; these must be addressed and responsibilities assigned to secure and protect the information that will consume, contain or divulge to downstream services. How systems are installed and maintained is covered in the Software Management Policy (EA-ISP-013[1]).

Please refer to the appendix for further explanation of the points below.

1. Authorisation and assessment

1.1 All new services and information systems or significant upgrades to existing provision of service must include authorisation and assessment prior to any:

- Acceptance into Service;
- and ultimately implementation

This authorisation and assessment should include:

Business approval	Senior Leadership Team or nominee approves the purpose and use of the system and ensures consistency with departmental strategy and any broader strategies if the system transcends the boundary of any single department.
Enterprise Architecture approval	Enterprise Architect or nominee to ensure alignment with architectural roadmap and prevention of service, system or functionality duplication across the business landscape.
Information security approval	Enterprise Security Architect or nominee to ensure the new or altered service or system complies with relevant information security policies and does not adversely affect the security of existing information architecture.
Technical approval	The Technical Architecture Team to ensure the service or system is sound from a technical perspective.

1.2 The information assets associated with any proposed new or updated service or system must be identified, classified and recorded, in accordance with the Information Handling Policy (EA-ISP-007[2]).

2. Service lifecycles

2.1 When requirements for new or upgraded services or systems are identified by the relevant Business Partners (BP) they begin the service development lifecycle, presented in figure 1 over leaf.

2.2 Throughout the development lifecycle, logical progression in enhancing business, technology, application and data layers become more defined prior to engagement with the physical work of actual delivery.

2.3 Enterprise Architecture Compliance reviews may be undertaken throughout development, however the final review must be performed before any upgrade or new service or system is accepted into service (through the Technology & Information Services Acceptance Into Service process).

[1] EA ISP 013 - Software Management Policy
[2] EA ISP 007 - Information Handling Policy

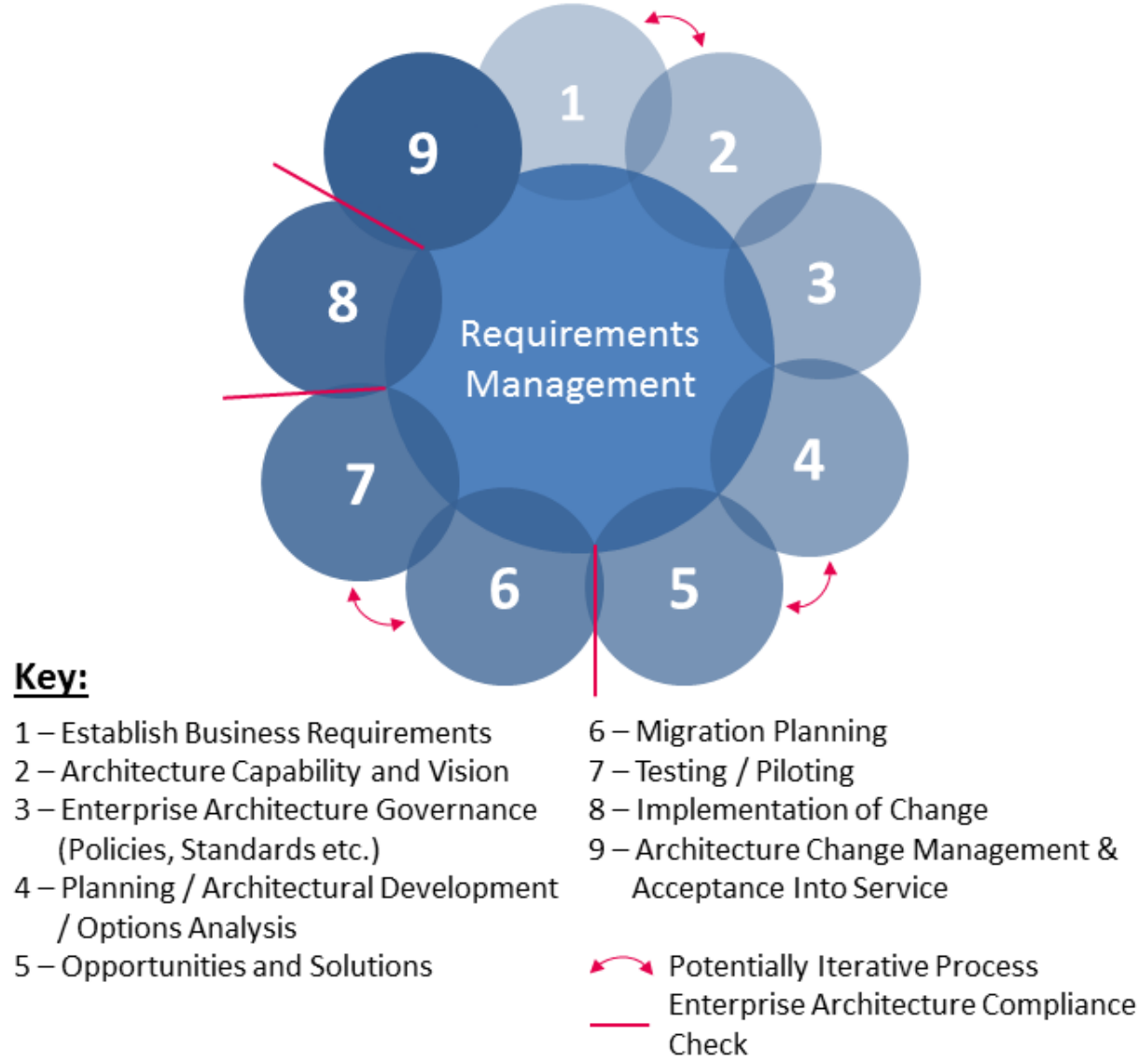

Figure 1 – Service development lifecycle

3. Equipment planning

3.1 Computer services and systems supporting business functions must be planned to ensure that adequate processing power, storage capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

3.2 Computer services or systems supporting business functions shall be given adequate protection from unauthorised access, environmental hazards and failures of electrical power or other utilities.

4. Service or system access

4.1 Access controls for all information and information services and systems are to be set at appropriate levels in accordance with the value and classification of the information assets being protected.

4.2 Access to operating system commands and application functions are to be restricted to those persons who are authorised to perform system administration or management functions. Use of such commands should be logged and monitored.

5. Implementation and testing

5.1 Prior to acceptance into the live (production) environment, all new or changed services or systems shall be tested by a variety of parties including (but not limited to):

5.1.1	TIS Delivery Manager or nominee	To provide assurance surrounding resilience, load balancing and other *stress* tests that may affect the performance of the system or service
5.1.2	TIS Enterprise Architect or nominee	To provide enterprise compliance checks for alignment with the architectural roadmap and agreed organisational strategies and policies; divergence from standard working practices and any mitigating measures required to allow service to be accepted into the live environment
5.1.3	TIS Enterprise Security Architect or nominee	To provide assurance surrounding compliance with information security policies, access control standards and requirements for ongoing information security management
5.1.4	User Acceptance Testing (UAT)	To provide assurance surrounding business capabilities of the system, service or product and ensure end users have a product that is fit for purpose and fulfils all known functionality requirements
5.1.5	TIS Acceptance Into Service (AIS) team or nominee	To collate documentation allowing the service to be understood, accepted and if required administered, alongside any appropriate routes for escalating problems by suitable members of the Service Management team

6. Succession planning

6.1 In order to ensure consistent and supported products are maintained within the organisation, it is essential that:

6.1.1 Services should be evaluated (even if very light touch) on a yearly basis review point to ensure that sufficient time is afforded to plan either an upgrade or replacement service or system to be sourced.

6.1.2 If an end of support or end of life date is issued by a manufacturer of a service or system or product in use within the organisation, it is the responsibility of all members of staff to notify the Strategy & Architecture team (within TIS) at the earliest available opportunity.

6.2 These points above will start the service development lifecycle to either detail the upgrade to the supported platform or source a replacement product that meets all of the business needs in an appropriate timescale.

Appendix

1. Authorisation and assessment

Explanatory Notes
A management authorisation process for new information processing facilities needs to be established and, where restricted (or sensitive) information might be involved, the business requirements for the development must specify the requirements for security controls.

Any new implementation or upgrade to an existing service or system where restricted (or sensitive) information is involved needs to be handled with care to ensure the continued integrity and confidentiality of information.

Information can be defined as data that has meaning. It is the meaning of this data which has to be protected or held confidential, in accordance with its worth to the organisation. As assessment of the risks to the organisation if information is altered, or seen by others may indicate that changes are needed to the service or system design, for example to improve the resilience or physical security of the service or system.

2. Service lifecycles

Explanatory Notes
Due to the diverse nature of the technology and products that are in use within the landscape of the organisation, it is imperative that planning, development, delivery, compliance and business needs are all realised prior to acceptance in the live environment.

No product, system or service will remain unchanged from first release until its official retirement. Monitoring throughout the lifetime of the entity will ensure sufficient time and resources are available to plan upgrades or to source replacements.

3. Equipment planning

Explanatory Notes
The capacity of all services or systems should be designed to ensure that the forecasted load can be supported and they must be engineered to minimise the impact on business processes of the inevitable faults and failures of system components.

The required service or system capacity is likely to increase over time due to increased processing load, software upgrades and other changes. Equipment should be designed with sufficient spare capacity to allow, within reason for these increases; if sufficient spare capacity is not a viable option then the scalability of the system must be assured to mitigate this concern.

Equipment must be sited or protected to reduce the risks of damage, interference and unauthorised access.

4. Service or system access

Explanatory Notes
Access control standards are the rules that an organisation applies to control access to its information assets. Such standards should always be appropriate to the organisation's business and security needs. High risk service or systems require more stringent access control safeguards due to confidentiality of the information they process and/or the purpose of the service, e.g. the funds

transfer systems used by banks. Ideally, the operating systems for such systems should be hardened to further enhance security. Duress alarms may be considered if there is a risk that operators will be subject to coercion. Access controls should extend to all information, including program source libraries, configuration files and back up files.

Operating systems are preloaded with commands and utilities which set up and maintain the computers environment. Applications and databases are delivered with tools to facilitate configuration or problem investigation. Services and systems should be hardened to remove all unnecessary development tools and utilities prior to delivery to end users. It is essential that the use of such system utilities is tightly controlled.

5. Implementation and testing

Explanatory Notes

Acceptance criteria for all services and systems should be established and tests carried out prior to acceptance into the live environment; these tests should be performed to ensure information security has not been jeopardised, that access control standards are met and that the risks identified during the various risk assessments have been addressed in the agreed way. It is also essential to ensure that systems are only accepted if the ongoing requirements of the Software Management Policy and the System Management Policy can also be met.

It is also essential to ensure that sufficient operating documentation is created to transition the service between test and production. This includes alignment with enterprise wide goals, business strategies, policies and working standards to ensure divergence from the roadmap is minimised.

6. Succession planning

Explanatory Notes

When a service, system or product transitions from main stream support to extended support, which usually means a reduced priority is afforded by the manufacturer to address security concerns. As this will affect software and hardware, a sufficient lead time will be required to find either a replacement solution and/or plan to upgrade must be started at the earliest available opportunity.