POL00337642

CIO Policies

Application Architecture Policy

Version – V1.1

POL00337642

CIO Policies - Application Architecture Policy

Contents

POL00337642

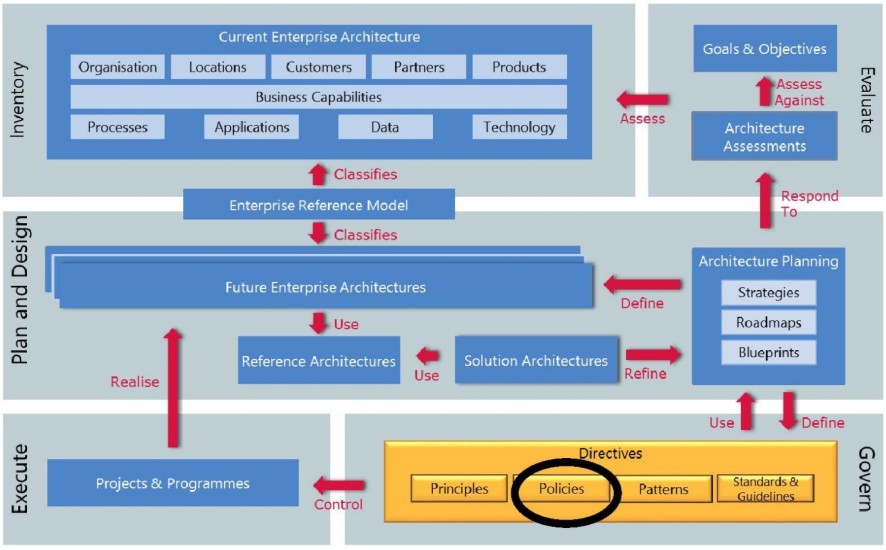
CIO Policies - Application Architecture Policy

1 Overview

1.1 The CTO deliverables framework

The CTO deliverables framework (see figure 1 below) describes the documentation that would be gathered to provide an overall description of an organisation and the impact of change upon it.

Architecture policies fit into the 'directives' section – the aim of which is to steer the strategic development of the architecture to the desired future state that meets the needs of Post Office business and IT going forward.



Documents produced as part of this framework, can be found in the Architecture Repository (see reference table in section 6)

Figure 1 – positioning of architecture policies in the EA Framework

Architecture policies build on the high-level Architecture principles enabling:

- Post Office and IT suppliers to comply with the principles when working at a detailed level
- Post Office design governance bodies (such as EAG and TDAs) to have sufficient information to measure designs against

1.2 Purpose of this policy

This Application Architecture policy defines the characteristics of 'applications' needed to meet the architecture principles, the way in which they interact and how they will be managed.

An 'application' in this context means the use of a technology, software downloaded onto a device and/or software-as-a-service. An application fulfils a purpose, or provides a 'service' to support one or more business processes and it (either independently or jointly) enables a business capability. Applications can be used as components or 'building blocks' of an application set, which is then referred to as a 'system'.

POL00337642

CIO Policies - Application Architecture Policy

1.3 Who must comply

This Application Architecture policy applies to all change programmes and projects that impact the Post Office enterprise architecture, including IT supply chain partners, with the exception of:

- 3rd party white-label partners who are developing Post Office branded products and services on their own platforms and for which they own the intellectual property (e.g. BOI)
- Partners for whom Post Office are effectively just 'hosting' their branded services (e.g. Moneygram)
- Joint ventures (e.g. FRES)
- Wholly owned Post Office subsidiaries (e.g. POMS)

1.4 How this policy impacts the application landscape

Please note that any application adopted by Post Office must be fully compliant to Procurement policies and meet Legal requirements (even if considered 'free'), especially where users sign-up to T&C's on behalf of Post Office. Please also refer to the Acceptable Use policy, which makes reference to acceptable use of software (see reference table in section 6)

1.4.1 Existing Applications

This policy can only be applied to new and upcoming application design, as many of the current ("legacy") application systems do not conform to the desired characteristics required by this policy

Evolution of legacy systems may also be possible by gradually "modularising" them, identifying their core functions and replacing them with common application services.

1.4.2 New Applications

New applications must conform to the stated characteristics. Where a number of applications combine to provide a service (or 'system'), in the situation where some are new and others are re-usable components that existed previously – only the new components are expected to comply.

Please follow the standard design approval process when new applications are needed, so that Procurement, EAs and Service Management are included in the decision making.

New applications that are being evaluated may be developed in-house, developed/ supplied by partners, or are trials of off-the-shelf packages or software, in order to assess the potential for specific technology capabilities required for Post Office in the future. This would include:

- Pilots
- Prototypes
- Proof of concepts
- Minimum viable products
- Software trials

POL00337642

CIO Policies - Application Architecture Policy

These all exist to confirm a hypothesis – i.e. to prove proposals and/or assumptions.

Systems selected in this way must conform to this Application Architecture policy, before being deployed for operational use. This is because development of this sort tends to be done in an evolutionary manner (test-and-learn basis) and, as such, may lack structure and/or operational documentation and may not be optimal in terms of support or future potential for growth/interoperability. There must therefore be an end date or evaluation date set for any trial and an expectation of some remediation work and/or approval process undertaken prior to 'go live' where needed for the system to conform to this policy

POL00337642

CIO Policies - Application Architecture Policy

2 Application Characteristics

Applications, as a part of our (and our customers' and partners') business processes, are critical components that must have the following characteristics to meet the architecture principles. Note that there will be additional characteristics required to meet security and data privacy requirements, which have not been included here, as they have been documented elsewhere (see reference table in section 6):

2.1 Portability

- Applications must be able to be hosted in any environment and accessed from any standard browser (where applicable)
- Application choices must avoid vendor and/or supplier lock-in. Ease of migration away at end of contract must be a key consideration in design.

2.2 Interoperability

- Integration between applications must not require one application to have any knowledge of what another does, thus reducing the risk that a change in one application/module will force a change in another

2.3 Scalability

- Any application should have the capability to be scaled for use across Post Office, unless it has been specifically designated as a niche application for a specific set of users only
- Individuals requiring access to applications must work with Procurement and Enterprise Architects to ensure that Post Office can capitalise on economies of scale, that we do not exceed licensing limits and that we understand which business capabilities are being underpinned by which application or system

2.4 Flexibility

- Applications should be capable of providing a service to potentially any Post Office user (which could be a person or another system, including external users/systems)

2.5 Usability

- Applications must conform with Post Office standards, which means that e.g. single sign-on can be applied so that application users do not have to remember multiple passwords and user ids
- It is also imperative that any contractual obligations and regulations around data location, support access and data protection are closely adhered to (see Information Protection policies and refer to Procurement)

POL00337642

CIO Policies - Application Architecture Policy

2.6 Manageability

- The life-cycle of one application service will be different to others. Being able to amend one without affecting the others leads to more cost effective ownership of systems and more exploitation of common services

2.7 Modularity (Loose-coupling)

- Loosely coupled services should be able to be joined together on demand to create composite services - or disaggregated just as easily into their functional components
- Modularity of applications and a business service-oriented set of application services will enable the rationalisation of applications, infrastructure, support and skills and minimise the impact of introducing a new application into the landscape

2.8 Published Interfaces

- Applications will use standard interfaces patterns for integration, as approved through Post Office design governance. Any exceptions or new interface spec or integration pattern will need to go through the appropriate governance

2.9 Service-based (Functional separation)

- Functionality within a system is logically separate, with well-defined roles and responsibilities, which do not overlap with other applications
- Application functionality will relate to specific layers of the architecture e.g. presentation, data, common services
- Application systems will not be built solely with one area of the business in mind (unless they are classified as providing specialised or niche functionality). Post Office will instead have a cohesive set of modular-based managed services that support application re-use and consequently a lower total cost of ownership for Post Office overall

POL00337642

CIO Policies - Application Architecture Policy

3 Application management and governance

3.1 Application Inventory

The CTO team will maintain a central Application Inventory 'master', with a view to having a common taxonomy across all areas of Post Office – from IT Security to Incident management and Procurement to Information Security (GDPR).

For home-grown applications, the CTO team will also maintain a Microservices/API Catalogue, to make it easier for people to find services already in place.

The Application Inventory and Microservices/API catalogue should hold, as a minimum, the following for each listing:

- Name
- Description
- Business Capability and/or Business Process it supports
- Business Owner/Unit responsible for paying for its use

Both documents are currently held in the Architecture Repository (see reference table in section 6), although the intention is to move the Application Inventory to Bizzdesign, so that there is a single version of the truth.

3.2 Application Assessment

The current application estate must be regularly assessed to ensure that Post Office technology remains cost-effective and fit-for-purpose, as well as understanding risk. This may also highlight opportunity for rationalisation and taking cost out of the IT estate.

The Post Office application architecture assessment will use the Gartner 'TIME' convention (tolerate, invest, maintain, exit), which will be calculated from a number of factors such as cost, age, criticality, supportability, functional fit etc.

This is likely to start from information that is readily understood (e.g. criticality) and evolve to include other factors (e.g. cost) that require links to other systems, such as Procurement.

3.3 Application Design Governance

This policy will be enforced through Application Design Governance. This operates on a number of levels within Post Office:

- A business goal or idea should start with engagement with Domain CTOs/EAs, so that the most appropriate solution guidance is given to meet the business need
- Having identified the right type of solution:
    - Requests for new device-based applications or software-as-a-service (SaaS) must start with a review of the Application Inventory (see section 4.1) to see what Post Office already has
    - Procurement must be engaged before approaching any suppliers (see reference table in section 6 for link to Procurement policies).

POL00337642

- Any need for a new application service to be built should start with a review of the Microservices Catalogue (see section 4.1) to avoid duplication and unnecessary spend
- In both cases the proposed design must go through the appropriate design governance to receive approval
- Requesting access to existing approved applications can be done via the software catalogue (see reference table in section 6)

New applications must then be added to the Application Inventory or Microservices catalogue as relevant, with the application assessment meta-data (as described in section 4.2) and accompanied by the associated application interface specifications

POL00337642

4 Minimum Control Standards

A minimum control standard (MCS) is an activity which must be in place in order to manage the risks so that risks remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types (i.e. directive, detective, corrective and preventive) which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

Risk Area: AP03 Manage the Enterprise Architecture

Risk Description: A common business architecture framework and methodology as well as an integrated architecture repository are used to enable re-use efficiencies across the business

The table below sets out how this policy helps implement the required controls (from the COBIT framework that has been applied to Post Office IT)

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	How this Policy helps Post Office meet the MCS
Develop the enterprise architecture vision.	The enterprise architecture is not fit for purpose and not supporting the business priorities.	AP03.02 Identify the enterprise goals and strategic drivers of the enterprise and define the constraints that must be dealt with, including enterprise wide constraints and project-specific constraints (time, schedule, resources, etc.). This is part of developing the architecture blueprint deliverable.	Enterprise Architects and Domain CTOs	Sets out the directives (constraints) that must be used when designing solutions
		AP03.05 Define what is inside and what is outside the scope of the baseline architecture and target architecture efforts, understanding that the baseline and target need not be described at the same level of detail.		Explains the scope of the application policy in terms of the current and future architecture

POL00337642

CIO Policies - Application Architecture Policy

		This is part of developing an architecture roadmap deliverable.		
		AP03.06 Confirm and elaborate architecture design principles. Ensure that any existing definitions are current and clarify any areas of ambiguity.		Explains how to apply the principles to the current and target architectures, including legacy applications and innovations
		AP03.10 Maintain an architecture repository containing standards, reusable components, modelling artefacts, relationships, dependencies and views to enable uniformity of architectural organisation and maintenance		The architecture policies form part of the information needed within the architecture repository
		AP03.25 Confirm scope and priorities and provide guidance for solution development and deployment		Describes the acceptable characteristics of the application architecture
		AP03.27 Manage architecture requirements and support with architectural principles, models and building blocks		Describes the requirements of the application architecture and provides practical information on how to apply principles to the application architecture

POL00337642

5 Policy Governance

5.1 Policy Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the Group Chief Information Officer (CIO) of Post Office Limited.

The Policy owner is the Group Chief Technology Officer (CTO) who is responsible for ensuring that the Architecture team conducts an annual review of this Policy and tests compliance across the Group. Additionally the Group CTO and the Architecture team are responsible for providing appropriate and timely reporting to the IT Leadership Board (ITLB).

The ITLB are responsible for approving the Policy and overseeing compliance.

5.2 Policy Version

Date	Version	Updated by	Change Details
27/11/2018	0.1-0.5	Matt Downey	Draft Version & updates
22/01/2019	1	Matt Downey	Released for approval
21/03/2019	1.1	Matt Downey	Baselined Formatting tweaks (removing 'draft' watermark, font sizes) and minor updates following reviews (latest framework diagram and moving text re involving Procurement para 1.4)

5.3 Policy Approval

Committee	Date Reviewed
ITLB	Feb 2019
EAG	19 March 2019

Group Oversight Committee: IT Leadership Board

Policy Sponsor: Rob Houghton – Group CIO

Policy Owner: Michael Austin – Group CTO

Policy Author: Matt Downey - EA

Next review: 10/02/2020

POL00337642

CIO Policies - Application Architecture Policy

6 Glossary & References

Term	Definition
'Post Office' or 'Group'	Post Office Limited and Post Office Management Services Limited (POMS)
COBIT	COBIT is an IT management framework developed by the ISACA to help businesses develop, organize and implement strategies around information management and governance
'application'	Use of a technology, software downloaded onto a device and/or software-as-a-service. An application fulfils a purpose, or provides a 'service' to support one or more business processes and it (either independently or jointly) enables a business capability
'taxonomy'	Common language or dictionary to ensure that applications/processes are referred to consistently, either by the same name or that different names can be cross-mapped to eachother for traceability

Reference	URL
Architecture Repository (holding policies, principles, standards, guidelines and taxonomies)	https://poluk.sharepoint.com/sites/Extranet/Strategy/AR/SitePages/Architecture%20Repository%20Home.aspx
Software Catalogue	https://fidm.access.it-solutions.atos.net/auth/Login?Template=PostOfficePasswordOnly&GAURI=https://portal.it-solutions.atos.net/group/postoffice%20%20%20
Data Privacy and security policies, including Acceptable Use	Key Policy Framework https://poluk.sharepoint.com/sites/thehub/SitePages/Key%20policies.aspx?web=1
Procurement Policies	https://poluk.sharepoint.com/sites/POA001/procurement/SitePages/Policy-and-Legal-Obligations.aspx?slrid=c50aa99e-d0c2-7000-1270-a69b7e2f9a35