System Implementation Policy

PHX054

Contents

Policy Statement

The objective of this document is to formalise the implementation of new systems and toolsets in Phoenix.

Intended Audience

This document is intended for all employees and interested parties in reference to corporate governance within Phoenix.

Consequences of Non-Adherence

Failure to adhere to this document may lead to disciplinary action as outlined in the Company Handbook.

System Implementation

As Phoenix evolves, new system and/or toolsets and ways of working will be required to ensure Phoenix stay innovative and productive. Although a great way of growing and developing our operations, the introduction of new systems, toolsets, applications, and software introduces increased business, security, and data risks as the data in our control is moved into systems and/or toolsets beyond the scope of Phoenix IT Infrastructure Management. When introducing a new system, the following steps need to be taken to ensure the systems and/or toolsets used are appropriately secure and resilient.

To ensure appropriate considerations are made, the following steps are in place:

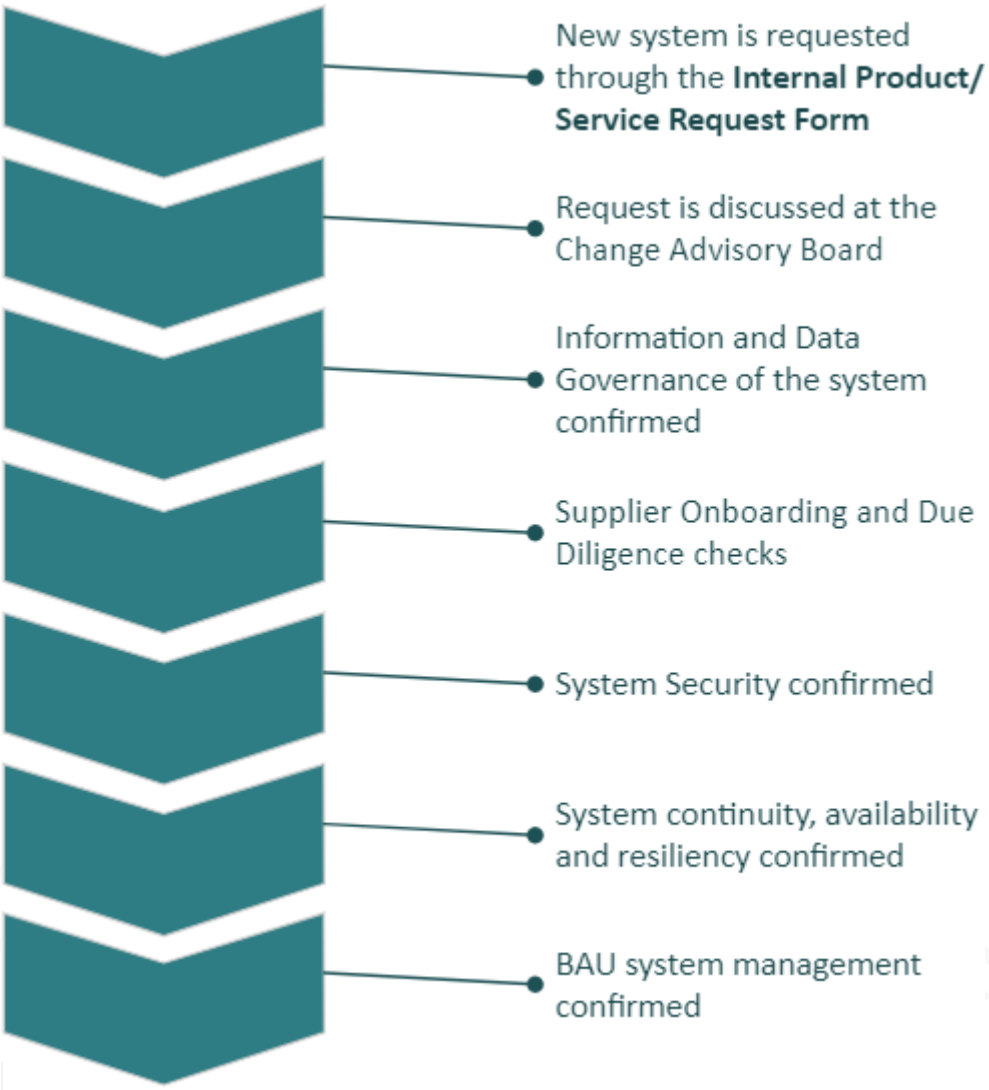

Figure 1 Systems and/or toolset Implementation Approval Steps

Change Advisory Board

The Phoenix Change Advisory Board (CAB) has representation from the IT Infrastructure Team; Development Team; Governance; Business Process and the Board. These individuals ensure no duplication of efforts takes place across the business and any changes implemented do not conflict with existing technology, compliance, or operational requirements.

The CAB meets once a week and confirms go-ahead for additional systems.

Information and Data Governance

Information and Data governance is primarily lead by the General Data Protection Regulation and the Data Protection Act 2018. Under the legal obligations required, Phoenix is required to

maintain Data Protection Impact Assessments (DPIA's) and Records of Processing Activities (ROPA's) available upon request to any data subject or customer organisation.

To ensure compliance, Phoenix is required to create, maintain, and review all data streams taking place throughout its operations to be able to accurately report back to individuals where their data is hosted, by whom, and for how long. This is also a requirement to accurately respond to are Subject Access Requests (SARs) and a data subject's Right to be Forgotten.

To meet these requirements, Phoenix must document what data is being processed, by which systems and/or toolsets, any processing taking place throughout the process, and be able to report on any third-party access to the data.

Provider Due Diligence

System and/or toolset providers must have contractual, financial and security agreements in place as per the Phoenix Supplier Onboarding Process to ensure quality systems are being utilised.

Systems and/or Toolset Security

To ensure the data within the systems and/or toolset is secure, basic security due diligence must take place on all systems and/or toolsets used within Phoenix activities. In line with ISO27001 Information Security Management and Cyber Essentials PLUS Security frameworks, consideration for systems and/or toolsets include:

- User Access
- Password Security
- Data hosting
- Penetration Testing
- Patching and Vulnerability Testing
- Secure coding
- Data in transit security
- Operations security
- Logging and monitoring
- Information backup

This provides assurance that systems and/or toolsets hosting data outside of the Phoenix estate and Infrastructure Management scope is managed to the same standard of systems and/or toolsets maintained internally, further lowering the risk of a data breach or security incident.

Phoenix remain liable for security incidents caused by third-party providers.

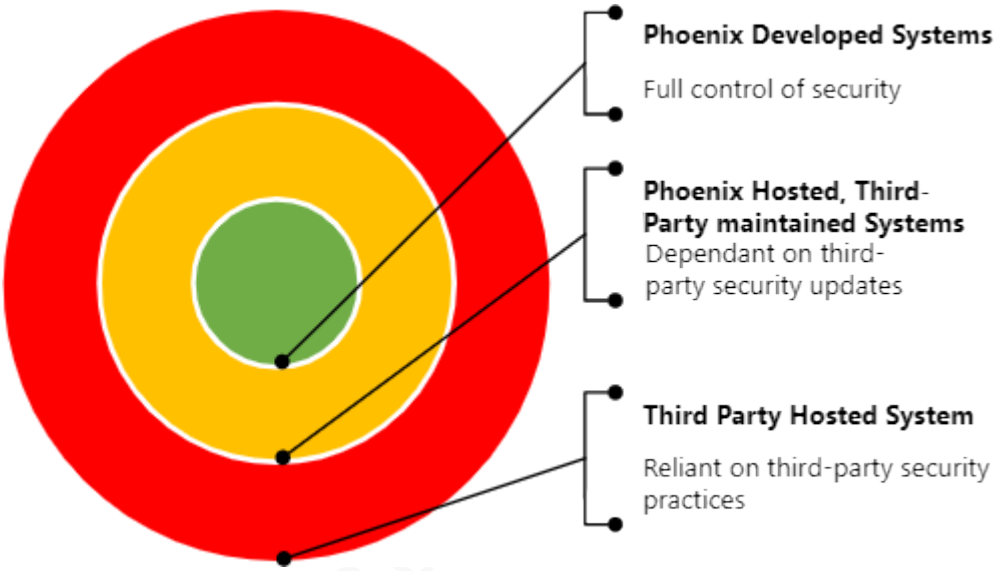

Figure 2: Phoenix Infrastructure Boundary and Risk Visualisation

Systems and/or Toolset Continuity, Availability, and Resiliency

Ensuring systems and/or toolset availability is essential for business continuity, therefore all systems and/or toolsets must be considered for Business Continuity Plans and Business Impact Assessments (BIA's).

Ongoing Systems and/or Toolset Management

Upon implementation, the roles, and responsibilities of systems and/or toolset maintenance need to be confirmed. This includes:

- Data is maintained and is accurate
- Data is deleted as required as per GDPR and DPA requirements
- User access is managed in line with the company's Joiners, Movers, Leavers procedures
- Security is maintained
- Phoenix remain compliant with any licencing requirements
- Payment schedules are maintained
- Any incidents involving the systems and/or toolset or toolset is reported appropriately.

The system must also be added to the Phoenix Service Catalogue maintained by the Service Desk.

Policy Governance

The following table identifies who within Phoenix is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Governance Manager
Accountable	Managing Director / Operations Director
Consulted	Directors, Service Management Committee
Informed	All Employees, Contractual Partners, and Third-Party Agents.

Review and Revision

This policy is reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the ISMS with any subsequent changes authorised by the Managing Director.

Version Control

Author	Version	Date	Description
ISC	1.0	28/06/2021	Original Document
ISC	1.0	09/08/2022	Annual review – no changes
ISC	1.0	03/08/2023	Annual review – no changes

Document Approval

Name	Version	Date	Position
Clare Metcalfe	1.0	28/06/2021	Operations Director
Clare Metcalfe	1.0	30/09/2022	Operations Director
Clare Metcalfe	1.0	10/08/2023	Operations Director

Signed:  Clare Metcalfe, Operations Director

Dated: 10/08/2023