Project Framework

February 2021

Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Description | Date |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 4](#_Toc64292408)

[2 Project Framework 5](#_Toc64292409)

[3 Business Case 6](#_Toc64292410)

[4 Business Case Review 8](#_Toc64292411)

[5 Design and Plan 10](#_Toc64292412)

[6 Design and Plan Review 14](#_Toc64292413)

[7 Build and Test 16](#_Toc64292414)

[8 Build and Test Review 20](#_Toc64292415)

[9 Deliver, Close and Maintain 21](#_Toc64292416)

[Appendix I: Simple Projects 24](#_Toc64292417)

[Appendix II: Change Windows 25](#_Toc64292418)

[APPENDIX iii: Project Template library 26](#_Toc64292419)

[APPENDIX IV: Project library 27](#_Toc64292420)

[APPENDIX V: GG Key Responsibilities 28](#_Toc64292421)

[APPENDIX VI: PMO Key Responsibilities 29](#_Toc64292422)

1. Introduction

Projects are started for a variety of reasons, but fundamentally they all seek to deliver a benefit to the firm. The benefit may be an efficiency, it may be compliance with a regulatory framework, or it may be a new service delivery. The benefits are numerous but to realise them, projects should be approached in a simple but structured manner. The structure is important because it ensures a consistent delivery approach and that project teams address all requirements as they progress from business case through to go live. The structure also provides the opportunity for consistent oversight and accountability which is essential given the business and financial impact that projects can have within a firm.

This document will define the project structure within the UKIME region, and will provide a guide to each stage of the process together with the associated documents and roles needed to complete them.

Before embarking on what might be a lengthy process, you will need to confirm that you are dealing with a project rather than a business as usual ("BAU") activity. Projects have very specific characteristics when compared to BAU activities and to assist you in determining whether you have a project or a BAU activity, the projects library has an assessment tool that can determine the status of your proposal.

If the proposed work is a project, you will need to decide whether you have a Simple or Complex project. Simple Projects have a short duration and are characterised by low risk, relatively low cost and a focus within a single functional area. (Appendix I). All other projects are classified as Complex Projects and must be delivered within the project framework and adhere to the reporting and governance arrangements appropriate for projects of this type.

To determine which project type you are dealing with please use the project assessment tool on the Projects Library.

1. Project Framework

The following diagram provides a high-level view of the project framework. Each stage of the framework has a number of roles, responsibilities, and work products associated with it, and these will be reviewed in subsequent sections.



1. Business Case
	1. Work flow



* 1. Purpose

The purpose of this process is to build a coherent business case that can fully describe a project, and to prepare the proposal for scrutiny by the Investment Governance Committee.

The business case template lists all the information needed before a business case can be submitted for consideration. In its simplest terms, the key points are:

* + What is being proposed?
	+ Why is it being proposed?
	+ What will the benefits be?
	+ How will be it delivered and by whom?
	+ What are the security considerations?
	+ How much will it cost and how long will it take?
	+ What are the risks and how will they be mitigated?
	+ How does the project fit with the UKIME Strategy 2021?

An additional consideration will be the global/regional project landscape. A project may be aligned with business strategies but has the proposed project been attempted elsewhere? Is it being implemented in another region which could impact licensing, resourcing or timelines? There needs to be due diligence to understand the potential impact that global/regional projects will have on the proposal.

Authoring the business case can be a challenging activity given the complexity of some projects, and therefore the PMO can provide guidance and help to support its preparation.

* 1. Roles and Responsibilities

The table below lists the roles needed to sign off a business case. For many projects such roles may be the responsibility of one or two people. The key point is that the business case needs to be prepared and signed off by those who have responsibility for ownership, budget and delivery.

***Please note that sign off does not mean acceptance for the project to be progressed to the design and plan phase. It means that key stakeholders agree that the business case has a level of completeness and detail that makes it ready for consideration by the GG.***

|  |  |
| --- | --- |
| Role | Responsibility |
| Budget owner | To sign off the proposed spend as documented in the business case.  |
| Project Manager | Prepare the business case with the assistance of the PMO if required. |
| Stakeholders | To sign off the business case. |
| Business owner | To sign off the business case and to assist in its production. |

* 1. Related ISO references for phase

|  |  |  |
| --- | --- | --- |
| Reference | Detail  | Related project artefact |
| A.6.1.5 Information security in project management | Information security should be integrated into the organization’s project management methods to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character. e.g. a project for a core business process, IT. facility management and other supporting processes. The project management methods in use should require that:* Information security objectives are included in project objectives;
* An information security risk assessment is conducted at an early stage of the project to identify necessary controls;
* Information security is part of all phases of the applied project methodology.
 | * Business case
* Project plan
* Risk log
* Resource plan
* Information Security Standard – System Development
* Information Security Standard Library
 |

1. Business Case Review
	1. Work flow



* 1. Purpose

The purpose of the business case review is to enable the Investment Governance Committee ("GG") to assess the proposed project and if approved, to allow the project to proceed to the next stage in the process.

The assessment will not just consider the merits of a proposal in isolation, it will consider the proposal within the context of the current project portfolio, any resource and budget constraints, and any global/regional project initiatives.

To assist the assessment by the GG, the PMO will compile a business case checklist. The purpose of the checklist is to provide assurance to the GG that the business case is complete, and that supporting contextual information is available.

* 1. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| PMO | * Collate relevant project information to support the business case submission.
* Complete the business case checklist.
* Update project list and portfolio report
 |
| GG | * Review the business case submission.
* Decide whether the business case should be approved, rejected or returned with a request for additional detail.
 |

1. Design and Plan
	1. Workflow



* 1. Purpose

The purpose of the design and plan phase is to transform the deliverables outlined in the business case into the solution design and plans that will enable the project to be completed within agreed timelines and costs.

During this phase attention must not be given exclusively to the system specification and the project plan. Time and thought must be given to how users will be introduced to the change, how, if appropriate, it will be supported following go live, and how the design and implementation will adhere to the firm’s security requirements. Consideration will also need to be given to timelines and costs.

The business case included time and cost estimates and approval to progress was based in part on those estimates. If timelines and costs are subject to material change following Design and Plan, additional budget approval may need to be sought from the budget holder, and the project may need to be re-approved by the GG.

During the Design and Plan phase, the Project Manager will need to keep the PMO informed on progress by submitting a monthly project status report.

* 1. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| Project Team | To author the required plans and specification documents. |
| Project Manager | To author the project planTo update the time and costs estimates and ensure that the PMO, GG, and budget holders are aware of the updates estimates.To ensure the timely sign off of any 3rd party contractsTo ensure that all required plans and specifications are completed and signed off.To update the PMO with status reports. To compile the design and plan checklist. |

* 1. Related ISO references for phase

| Reference | Detail  | Associated project artefact |
| --- | --- | --- |
| A.6.1.5 Information security in project management | Information security should be integrated into the organization’s project management methods to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character. e.g. a project for a core business process, IT. facility management and other supporting processes. The project management methods in use should require that:* Information security objectives are included in project objectives;
* An information security risk assessment is conducted at an early stage of the project to identify necessary controls;
* Information security is part of all phases of the applied project methodology.
 | * Business case
* Project plan
* Risk log
* Resource plan
* Information Security Standard – System Development
* Information Security Standard Library
 |
| A.18.2 Compliance | To avoid breaches of contractual obligations related to information security and of any security requirements. | * Master services agreement
* Statement of Work
* Risk Log
* Project plan
 |
| A.13.2.4 Confidentiality or non-disclosure agreements | Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, regularly reviewed and documented. | * Supplier NDA
 |
| A.15.1.1 Information security policy for supplier relationships | Ensure the existence of a data-sharing agreement that clearly delineates roles and responsibilities. Some data privacy regulations may have specific data sharing requirements that must be met | * Master services agreement
 |
| A.15.1.2 Addressing Security Within Supplier Agreements | To ensure the protection of the organization’s assets that are accessible by suppliers. | * Master services agreement
* Statement of Work (SoW)
 |
| A.15.2 Supplier service delivery management | Maintain, in compliance with supplier agreements, an agreed level of information security and delivery of service. | * Master services agreement
 |
| A.18.1.4 Privacy and protection of personally identifiable information | The project should adhere to the data policy written and implemented to protect privacy and personal identifiable information.  | * Technical solutions that address functional and non-functional requirements.
* Risk log
 |
| A.14.1.2 Securing application services on public networks | The information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. | * Technical solutions that address functional and non-functional requirements.
* Risk log
* Information Security Standard
 |
| A.14.2.1 Secure development policy | Rules for the development of software and systems should be established and applied to developments within the organization. | * Information Security Standard – System Development
* Project plan
 |
| A.9 Access control | Control relates to the business requirements of access control. | * Technical solutions that address functional and non-functional requirements.
* Risk log
* Foundational standards within the Information Security Standard Library
 |
| A.14 System acquisition, development and maintenance | Ensure that information security is an integral part of information systems across the entire lifecycle | * Foundational standards within the Information Security Standard Library
* Project plan
 |
| A.14.2.3 Technical review of applications after operating platform changes | When operating platforms are changed, business-critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. | * Assessment of current operational status
* Project plan
* Test plans
 |
| A.14.2.5 Secure system engineering principles | Design principles encompassing information security related to:* business layer – e.g., based on user authentication level; only particular users can see personal data
* data layer – e.g., only logging in with a strong database password for database maintenance activities is allowed
* applications – e.g., application encryption is used for data export and import
* technology – e.g., open-source software and state-of-the-art hardware and network infrastructure provided by selected vendors are used
 | * Technical solutions that address functional and non-functional requirements.
* Information Security Standard
 |
| A.14.2.6 Secure development environment | Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. | * Information Security Standard
 |

1. Design and Plan Review
	1. Work flow



* 1. Purpose

The purpose of the Design and Plan review is to provide assurance that the project team have considered all relevant aspects of the project and are ready to commence the Build and Test phase.

The review will focus on material changes to the details outlined in the business case e.g. time, costs, resourcing, approach, risk, and on ensuring that the project has been thoroughly considered and planned.

If there are significant changes to costs, timescales, or design, the GG will request amendments to the design and plan, or will request a re-submission of the business case based upon the new information.

* 1. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| PMO | To collate submitted Design and Plan checklists and to circulate them to the GG prior to the monthly meetings. Inform project teams on the next step decision |
| GG | Review Design and Plan checklistsDecide on the next steps  |

1. Build and Test
	1. Work flow



* 1. Purpose

The purpose of build and test is to produce the deliverables outlined in the business case using the plans and specifications authored during the Design and Plan phase.

* 1. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| Project Team | To produce the deliverables outlined in the business case.To ensure that appropriate testing is completed as defined in the test plan and that the deliverables are signed off as ready to deploy to live. |
| Project Manager | To mobilise resources when requiredTo ensure that the project is delivered within a structure defined by the project plan.To ensure that risk and issue logs are maintained and that appropriate mitigation plans are enacted. To ensure that monthly project reporting is completed as expected and received by the PMO.To ensure that planned communication activities are completed on schedule.To ensure that service transition, change management and handover activities are planned and ready to action.To monitor time and costs and to highlight when they are likely to exceed budgeted amounts.  |

* 1. ISO References for phase

| ISO Reference | Detail | Associated project artefact |
| --- | --- | --- |
| A.14.3.1 Protection of Test Data | Test data should be selected carefully, protected and controlled. | * Information Security Standard Library
* Test plan
* Project plan
 |
| A.14.2.9 System Acceptance Testing | Acceptance testing programs and related criteria must be established for new information systems, upgrades and new versions. For acceptance testing, the tests and the criteria for demonstrating a successful test should be designed and developed based on business requirements prior to tests being carried out. Acceptance testing should also include security testing | * Test plan
 |
| A.14.2.8 System Security Testing | Testing of security functionality needs to be carried out during development. Specific testing of security functionality for any development must be carried out and signed-off by an appropriate authority with security competency and responsibility | * Test plan
 |
| A.14.2.3 Technical Review of Applications After Operating Platform Changes | When operating platforms are changed, business-critical applications need to be reviewed and tested to ensure there is no adverse impact on organizational operations or security. | * Test plan
* Project closure report
* Assessment of current operational status
* Project plan
 |
| A.6.1.5 Information security in project management | Information security should be integrated into the organization’s project management methods to ensure that information security risks are identified and addressed as part of a project. The project management methods in use should require that:* Information security objectives are included in project objectives;
* An information security risk assessment is conducted at an early stage of the project to identify necessary controls;
* Information security is part of all phases of the applied project methodology.
 | * System solution design
* Test plan
* Project plan
* Risk log
* Resource plan
* Information Security Standard
 |
| A.18 Compliance | To avoid breaches of contractual obligations related to information security and of any security requirements. | * Statement of Work
* Risk Log
* Project plan
 |
| A.18.1.4 Privacy and protection of personally identifiable information | The project should adhere to the data policy written and implemented to protect privacy and personal identifiable information.  | * System solution design
* Risk log
 |
| A.18.1.3 Protection of records | Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements. | * System solution design
* Risk log
 |
| A.14.1.2 Securing application services on public networks | The information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. | * System solution design
* Risk log
 |
| A.14.2.1 Secure development policy | Rules for the development of software and systems should be established and applied to developments within the organization. | * Information Security Standard – System Development
* Project plan
 |
| A.9 Access control | Control relates to the business requirements of access control. | * System solution design
* Risk log
 |
| A.14 System acquisition, development and maintenance | Ensure that information security is an integral part of information systems across the entire lifecycle | * Foundational standards within the Information Security Standard Library
* Project plan
* Change requests
* Communication plan
 |
| A.14.2.5 Secure system engineering principles | Design principles encompassing information security related to:* business layer – e.g., based on user authentication level; only particular users can see personal data
* data layer – e.g., only logging in with a strong database password for database maintenance activities is allowed
* applications – e.g., application encryption is used for data export and import
 | * System solution design
* Information Security Standard - System Development
 |
| A.14.2.6 Secure development environment | SD 1.21 text | * Section SD2.5 System Testing within Information Security Standard – System Development
 |
| A.15.1.2 Addressing Security Within Supplier Agreements | To ensure the protection of the organization’s assets that are accessible by suppliers. | * Master services agreement
* Statement of Work (SoW)
* Risk log
 |
| A.15.2 Supplier service delivery management | Maintain, in compliance with supplier agreements, an agreed level of information security and delivery of service. | * Master services agreement
* Project plan
* System solution design
* Risk log
 |
| A.18.1.3 Protection of records | Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements. | * Technical solutions that address functional and non-functional requirements.
* Risk log
 |
| A.14.2.2 System change control procedures | Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures. | * Change Log
* Project RFC
* Decisions Log
 |

1. Build and Test Review
	1. Workflow



* 1. Purpose

The purpose of the build and test review is to give the GG assurance that the project team have completed all necessary tasks in readiness for a deployment into the live environment.

Critical to the success of any project are those service transition activities that move it from the test environment into business as usual environment, and the GG will need confidence that all relevant activities have been considered and planned for.

* 1. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| Project Manager | To ensure that all relevant service transition activities have been planned and signed off.To complete the Build and Test checklist |
| PMO | To review the information from the PM and to recommend the next course of action to the GG.  |
| GG | To approve the transition of the project into production |

1. Deliver, Close and Maintain
	1. Workflow



* 1. Purpose

The purpose of the deliver, close and maintain phase is to ensure that the deliverables outlined in the business case, and built during the build and test phase, can be deployed to live using a planned approach that minimises risk and disruption to other services.

Once the GG approves the go live, the following three key activities commence:

* The PMO updates relevant project documentation and informs relevant global /regional bodies on the go live.
* The training and communication activities planned to support the go live.
* The activities related to the actual go live. Change management processes need to be adhered to and the change needs to scheduled taking into account the change windows (Appendix III) and any other planned activities.
	1. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| Project Manager | Ensure that the project completes all necessary change control processes and that agreed go live dates are communicated to the project team and the users.Ensure that training and communication events complete as planned.Ensure that the project is signed off as completed and closed by business sponsor. Ensures that the service catalogue is updated.Ensures the completion of the change request needed to support the go live review by the change board |
| PMO | Updates project portfolio and project listUpdates global/regional bodies with the project go live |
| Change board (CAB) | Assesses the go live change request and agrees on a go live date.  |

* 1. ISO References

|  |  |  |
| --- | --- | --- |
| Reference | Details | Related Artefact |
| A.14.2.2 System change control procedures | Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures. | * Build and Test check list
* CAB (RFC)
* CM Risk Matrix template
* Communication plan
 |
| A.14.2.3 Technical review of applications after operating platform changes | When operating platforms are changed, business-critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. | * Assessment of current operational status
* Project plan
* Test plans
* Project close report
 |
| 8.1 Operational Planning and Control | Clause 8.1 requires a demonstration of processes controlling critical security-related activities. Some mechanisms to assist with conformance to this subsection include:* The use of documented security plans or security calendars;
* Monitoring and controlling changes to the environment;
* Implementing controls around third-party outsourcing arrangements.
 | * Service Transition plan
* Project plan
* Build and Test check list
* CAB (RFC)
* CM Risk Matrix template
 |

Appendix I: Simple Projects

A Simple Project is a small-scale project that can be approved by a functional lead. These projects also have a slimmed down delivery appropriate for work of this type.

It is important to note that Simple Projects cannot be used as a vehicle for introducing change whilst avoiding the more comprehensive structures of a Complex Project. Simple Projects must have a fully defined scope, cost, timescale and resource requirement. If a Simple Project requires a change of scope such that it would require review by the GG, the project will be suspended whilst it is presented to the GG for their consideration.

The workflow for a Simple Project is defined below:



Appendix II: Change Windows

The following table lists the change windows during which changes can, or can't be applied.

|  |  |
| --- | --- |
| Period | Description |
| Christmas/new year | Unless business critical, no changes will be applied during this period. |
| Year-end / month end | No changes can be applied to finance related systems e.g. PMS, Time recording, chrome river etc. – need a list, x days before and after month end. |
| Every Saturday night | Maintenance window for system changes, system reboots etc. |

APPENDIX iii: Project Template library

All project templates are stored within the Project Templates folder of the Projects portal site.

The library comprises the following templates:

* Build and Test checklist
* Business Case Check List
* Business Case
* CM Risk Matrix template
* Communications Plan Template
* Design and Plan Checklist
* Meeting agenda template
* Project Change Log
* Project Closure Report
* Project Issue Log
* Project Monthly Update
* Project Plan Template
* Project Proposal
* Project RFC
* Service Transition Plan
* Simple Project Monthly Update
* Simple Project plan
* Test plan
* Weekly project update

APPENDIX IV: Project library

All new projects will have a project team site set up which will store all project documents.

As a minimum, the project site must contain the following documents:

* Plans
	+ Project plan
	+ Test plan
	+ Risk/Issue log
	+ Communication plan
	+ Service transition/go live plan
* Business case/Project proposal
* Status Updates
* Project approvals

APPENDIX V: GG Key Responsibilities

The Governance Group is responsible for:

* Assessing proposed projects to ensure that they:
	+ Are well-thought-out,
	+ Meet global/regional strategic/operational business goals,
	+ Deliver value to the firm,
	+ Do not replicate capabilities within the existing technology portfolio
	+ Reflect budget and resource constraints
	+ Recognise risks and have appropriate mitigation activities.
* Undertaking an end to end project oversight including authorising progress through the project stages

The Investment Governance Committee is accountable for:

* All projects planned and delivered within UKIME region
* All project spend within UKIME region
* Ensuring that global and regional corporate bodies are informed about project status, go live activities, and the project pipeline.

APPENDIX VI: PMO Key Responsibilities

The PMO is responsible for:

* Collating project documents to present to the GG including:
	+ Current budget status
	+ Build and Test review documents
	+ Design and Plan review documents
	+ Business cases, including the business case check list, for proposed projects
	+ Project portfolio status report
* Updating the project portfolio status report
* Updating the UKIME projects list
* Maintaining the project library site
* Confirming completion of project stages
* Providing guidance on the authoring of project documents
* Dissemination of project information to relevant global and regional bodies.