Programme and Project Management Centre of Expertise

The Scottish Government
Riaghaltasna h-Alba

Independent Assurance

ICT Technical Assurance - A guide for Review Teams.

October 2014 V2.0

Contents

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to provide guidance to ICT Technical Assurance Reviewers and to inform those who will be reviewed an idea of what is likely to be covered.

ICT Technical Assurance will provide specific technical assurance as ICT projects progress through their lifecycle. It provides evidence-based technical findings upon which relevant governance bodies can make key decisions at investment, development and implementation milestones. ICT Technical Assurance can be used to support other Independent Assurance e.g. Gateway or can be stand-alone. This document therefore provides guidance for both scenarios but may not be needed in totality. The guidance supports the overall ICT Assurance Framework.

It is further designed to support Accountable Officers (AOs) and Senior Responsible Owners (SROs) in ensuring that proposed investment in ICT is strategically aligned with *Scotland's Digital Future: Delivery of Public Services.*

1.2 Why is ICT Technical Assurance Required?

There have been a number of well publicised ICT failures and cost escalations. ICT Technical Assurance is designed to ensure proposed technical solutions will meet user and business needs.

ICT Technical Assurance is intended to complement the Scottish Government's Independent Assurance Review process and provide a framework to drill down into technical aspects of projects to a greater depth than would typically be done by independent project assurance reviews. It ensures on-going strategic alignment and informs the technical wisdom of ICT investments in an ever-changing risk environment.

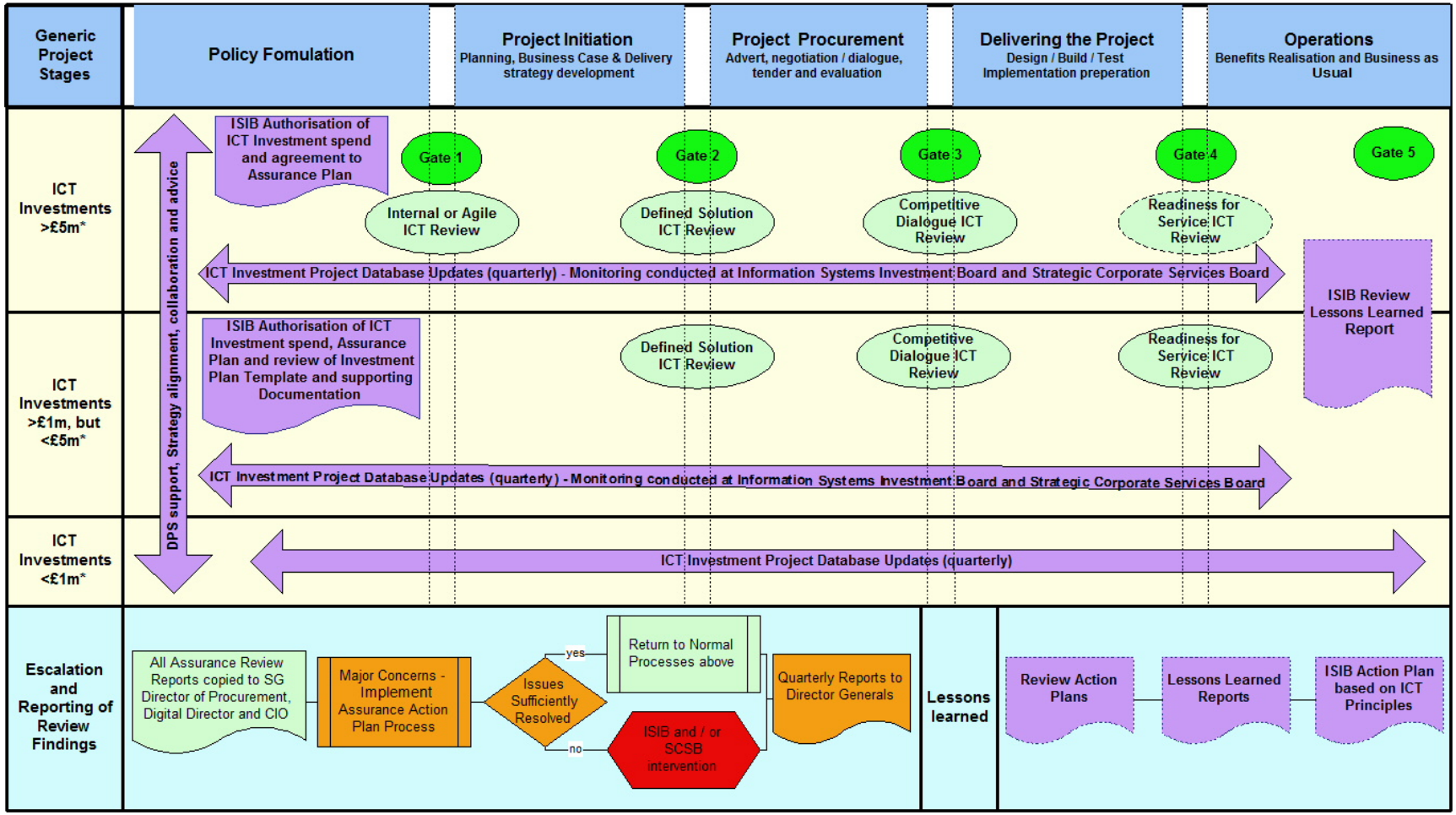
ICT Assurance recognises that a Delivery Strategy may be to contract with a supplier(s) or to build in house – and a number of variants in between. It recognises that an Investment Decision is not necessarily the signing of a contract(s) but may legitimately be the decision to invest internal resources on the development of an ICT solution to a business requirement.

In short, ICT Technical Assurance is required to give more technical focus to the assurance plans for projects and programmes with a high degree of ICT content

1.3 ICT Assurance Framework: From Policy To Operations

The diagram below illustrates the fit of ICT Assurance with the Scottish Government's Independent Assurance Review Process.

Central Government Assurance Framework for ICT Investment Projects



Gate 0 = Strategic Assessment
Gate 1 = Business Justification
Gate 2 = Delivery Strategy
Gate 3 = Investment Decision

Programme and Project Managemnt Centre of Expertise Managed Processes

Digital Public Service Managed Processes

Notes

* Definitions of ICT investments is based on the whole-life cost of implementation of the ICT aspects of projects. Where there are organisational capacity, size, capability or timescale issues or "leading-edge" technology requirements, there will be increased project delivery risk, the project will be subject to a higher degree of assurance.

There is a mandatory requirement to carry-out one ICT Technical Assurance Review, scheduling dependant on type of development. Further reviews likely to be beneficial. SRO / AO's have responsibility for providing Assurance over their Projects and the assurance can be met through other sources.

Whilst Gates and ICT Reviews are scheduled together above this is unlikely to happen in practice. There is opportunity to combine reviews or to use one type of review to inform the other.

2.0 ROLES AND RESPONSIBILITIES

2.1 Senior Responsible Owner (SRO) and Accountable Officer (AO)

Governance and Assurance processes for the Management of IT Investments remains the responsibility of the SRO and Accountable officer. It is necessary as part of this role to ensure that the technical solution will meet the business need and fits with the ambitions of the DPS strategies.

2.2 Programme & Project Centre of Expertise (PPM-CoE)

Support is provided by Scottish Government's Programme and Project Management Centre of Expertise (PPM-CoE) to AOs and SROs who obtain suitable reviewers as part of Independent Assurance.

2.3 ICT Assurance Review Team

The ICT Assurance Review Team will be Independent Assurance Reviewers, with appropriate ICT technical knowledge and experience.

The ICT Assurance Review Team will uphold the same brand values as Independent Assurance; namely to perform against an agreed Code Of Conduct, deliver a quality short report in real time based on evidence from interviews and documentation, and to maintain the principle of no surprises by keeping the SRO/AO or ICT Lead engaged throughout.

An ICT Assurance Review will typically be a two person team for two days, preceded by a planning day and pre-reading. This may vary according to complexity and risk profile.

3.0 AREAS TO PROBE AND DOCUMENTARY EVIDENCE

This section of the ICT Assurance Review guidance provides a checklist of topics that reviewers should probe during interviews and seek documentary support for. The areas to probe are structured around the general Scottish Government's PPM Principles but with a particular perspective to the ICT Technical environment. It is not intended to be a complete list but to act as an indicator as to areas Reviewers should probe.

3.1 Governance

3.1.1 Appropriateness and Empowerment

- Is the ICT elements suitably represented and appropriate in the level of governance related to levels of risk, cost and business change impact presented by the project?
- Are industry standard methods of ICT governance being used (e.g. ITIL Change Advisory Board etc)?
- Is the ICT project recognised as a component of a business-driven requirement, or is it an infrastructure refresh?

3.2 ICT Business Case Contribution

3.2.1 Strategic Alignment

- Has the project conducted an assessment against the published Digital Strategies (Digital Public Service: National Strategy, Central Government Strategy, High Level Operating Framework)?
- Has this assessment been used as a key component of the related business case (typically the Strategic Case section)?
- Has due consideration been given to the Digital future?
- Is the ICT system being deployed to replace an existing technology-based process or to migrate from manual to digital?
- Is there evidence of innovation in the project to ascertain the potential for migrating away from manual processes?
- Has due consideration been given to reduction of data storage and consequent need for data centres?
- Has the project developed an Information Handling Model (IHM), not only for the purposes of security but also data integrity, collection, storage, sharing and reporting?

3.2.2 Structure and Use

- Have the ICT components of the project been specifically identified for the contribution they make to project benefits?
- Has there been a rigorous analysis of each ICT technical option, and the rationale behind each, to fulfil the outcomes required from the project?
- Has the risk profile of the project been considered in the context of the different technologies being deployed?
- Has the organisation's Technical Design Authority (or Technical Architect, or equivalent) been involved in the creation and/or approval of the business case?
- Are the technologies being proposed bleeding edge, leading edge, stable and established or end-of life? What are the implications for integration, partnership working and what is the expected residual lifetime of the technologies once implemented?
- How much market competition is available for the proposed technologies? Has this been sufficiently explored in the Commercial Case?
- Are the dependencies between the ICT components and the business change components of the Business Case well documented and are they understood by approvers?
- What are the Business Continuity requirements – is there a Business Continuity Plan?

3.2.3 Sourcing, Build & Procurement

- Has reuse been considered before buy and buy considered before build.
- Has the project considered a range of procurement options and assessed the most appropriate route to market i.e. existing collaborative framework, Procurement Shared Service, collaborative procurement with other project teams/organisations, standalone contract.
- Has the project considered sustainability and taken into account the life-cycle of the requirement from design and manufacture to disposal and recycling.
- Have the available procurement routes (i.e. Restricted, Open, Competitive Dialogue etc.) been considered and assessed.
- Has the project undertaken any early market engagement activity with industry and suppliers to establish the availability of capacity and market views to the proposed requirement and procurement route.
- Where relevant to the requirement, has consideration been given to the use of Open Source and Open Standards.
- Are the application technologies used current, appropriate for the environment, fit for purpose and future proof?
- Do the user interfaces comply with all Legislative, Organisational and Best Practise accessibility and usability requirements?
- What plans does the project have to measure user satisfaction, not only with the end system when delivered, but also with their continued engagement during development?

- Has appropriate analysis been undertaken to assess the merits of in-house build, outsourced build or COTS/GOTS (Commercial/Government Off The Shelf) solutions?
- If so, is the procurement mechanism in place and are there likely to be any problems sourcing the required supply of skills at an acceptable cost?
- If the project is in-house development, have any implications for software licensing been considered?
- If the solution is in any way bespoke, have the implications for downstream support been considered? – Does an Operational Support Model document (or equivalent) exist.
- Has the project team engaged the correct level of specialist procurement/contract management expertise? (i.e. not just the generic purchasing department)
- Has IT specialist legal advice been engaged to advise on aspects of Intellectual Property Rights and contract Terms & Conditions?
- Is the project sufficiently specific about requirements to enter competition and subsequent contract and avoid un-planned-for costs?
- Is the project team putting sufficient focus into the support contract as well as the acquisition contract? Will both contracts be signed simultaneously? ?

3.3 Roles and Responsibilities

3.3.1 ICT Roles and Responsibilities

- Are roles and responsibilities clearly defined and understood
- Are decisions being taken by the correct people – e.g. responsibility for decisions on requirements/functionality are being taken by the business and not delegated to BAs/ICT
- Is there separation between roles – e.g developers are not undertaking system testing and UAT is not being undertaken by supply side.

3.4 Benefits

- Has the project conducted an assessment against the published Digital Strategies (Digital Public Service: National Strategy, Central Government Strategy, High Level Operating Framework)?
- Are benefits clearly stated
- Is there a clear understanding of the outcomes to be delivered by the programme and how the project will deliver these? Are they soundly based?
- Are the critical success factors agreed with stakeholders, still valid and can they be both quantified or measured
- Are there effective systems and plans for measuring, tracking and evaluating the realisation of benefits
- Are the main outcomes and desired benefits linked to strategic outcomes and to the deliverables from specific projects.
- Is there clarity on how the objectives from the ICT element link to the outcomes of the programme.

3.5 Risk

- Have the major risks been identified, understood, evaluated and considered?
- How will risks be managed?
- Is there a contingency plan and, where appropriate, business continuity plans?
- Have the risks for each of the options been evaluated?
- Have the risks for the preferred option been fully assessed?
- Has the project assessed whether it is breaking new ground in any areas?
- Should the project be broken down into a series of small steps or deliverables?
- Are there risk management plans?
- Have all the issues identified been satisfactorily resolved?

3.6 Planning

3.6.1 Data Integration

- Is the system stand-alone or will it be integrated with other systems?
- Has the data-flow between systems been mapped?
- Are both physical and logical data models available.
- Has it been agreed which systems will be treated as master and slaves?
- Has the business defined its detailed business processes and the role the systems play in those processes, including data input, maintenance and reporting?
- What is the provision for Business Intelligence Reporting
- Is Data Ownership clearly defined
- Are Data Sharing arrangements agreed and documented
- Has data to be migrated from one (or more) old systems. Is there provision for rollback. If no migration, what is the provision for the legacy systems.
- What are the backup strategies.

3.6.2 Security Accreditation

- Does the system require security accreditation?
- Will it be connected to a classified system or contain sensitive information?
- What level of security accreditation is required?
- Has a Risk Management Accreditation Document Set (RMADS) been completed?
- If accreditation is required. Has a CESG Listed Adviser Service (CLAS) Consultant been engaged? If not, has the lead-time to engage one been built into the project schedule?
- If the system is classified for national security, is CESG required to provide signoff? Has the lead time for this been built into the project schedule?

- If the system is to be connected to Government Secure Intranet (GSI), has the project produced a statement of compliance with the Code of Connection (CoCo)?
- Has the organisation's Senior Information Risk Owner (SIRO) given signoff to development at key stages?
- Is the system compliant with organisational standards e.g. COBRA

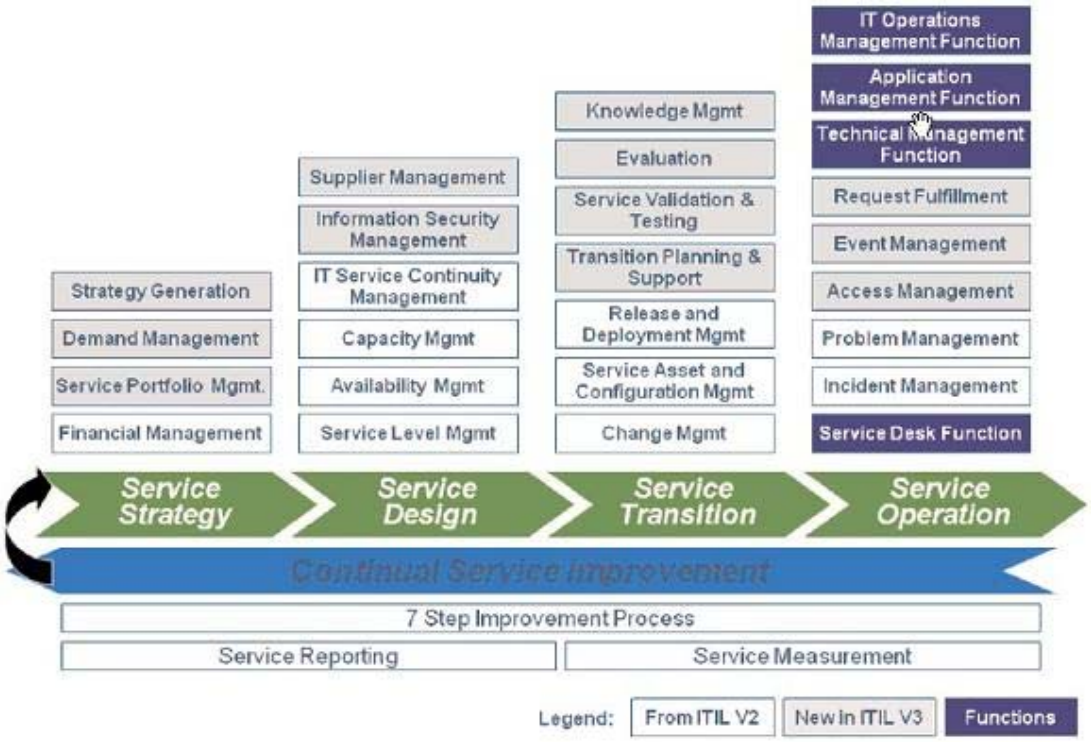
3.6.3 Project Implementation – System Rollout

- Does a full system rollout plan exist?
- Have the necessary client-side resources been identified and allocated to the required timings?
- Is the system go-live a big bang or incremental? Have the organisation's live services organisation been involved in planning and are they prepared?
- Is there any impact on outsourced live services provision? Is there a contract variation or any financial impact? Have these been authorised?
- What is the degree of sensitivity between the contracted rollout plan and client-side role? Would the client's failure to perform their part of rollout trigger a contract exception (sometimes referred to as a relief event or compensation event)? What would be the financial value of such an occurrence and has this been included in the risk register with appropriate mitigation?
- Is the project exercising appropriate change control, both contractually and technically?
- If the system implementation requires business change (this could be process, organisational or attitudinal), has a business change plan been linked to the system implementation?

3.6.4 Service Management Framework Alignment

- Has the project team conducted an assessment of the impact the project will have on the key elements of the IT Infrastructure Library (ITIL) v3 framework?
    - **Service Strategy**. How to transform IT service management into a strategic business asset. [This would be a major area of focus around Gateway 1 – Business Justification (and 0 – Strategic Assessment)]
    - **Service Design**. How to design IT services, processes and functions to realise the strategy. [This would be a major area of focus around Gateway 2– Delivery Strategy, and Gateway 3 – Investment Decision]
    - **Service Transition**. How to move new and changed IT services and components into a production environment safely and effectively . [This would be a major area of focus around Gateway 4 – Readiness For Service]
    - **Service Operations**. How to efficiently and effectively deliver and support IT services. [This would be a major area of focus around Gateway 4 – Readiness For Service and Gateway 5 – Business Operations and Benefits Realisation]
    - **Continual Service Improvement**. How to monitor and measure IT service management and make adjustments to remain aligned with business and strategy. [This would be a major area of focus around Gateway 5 – Business Operations and Benefits Realisation]

- Has the project team included the assessment (on a respectively sliding scale) of the five elements above at Gateway Reviews 1-5 or similarly timed ICT Assurance Reviews?
- Has the project team produced a plan to fill any gaps identified in the above assessment? As an example, the diagram below illustrates one suitable framework for assessment:



3.7 Resource Management

3.7.1 Project Resources

- Has the project developed a fully profiled resource requirements plan, detailing the ICT skills, numbers and timings of key resources for the project?
- If the project is in-house development, will additional skills need to be bought in?
- Has the project put in place a resource acquisition plan, to ensure that ICT skills are allocated internally or sourced externally?
- Has the project identified critical ICT resources, their key dependencies and links to contract obligations and put in place necessary risk mitigations?
- Will the business own sufficient skills to maintain the system?
- Are in-house ICT staff confident with the technologies used.
- Is there an appropriate balance between in house staff and contract staff.
- Are there formalised arrangements for skills transfer to skill up in-house staff

3.7.2 Technical Resources

- Are the existing technologies, environments and infrastructure capable of supporting the system
- Are suitable plans and financing in place to acquire any additional technologies, environments or infrastructure.
- Do the technologies support accessibility requirements.
- What are the Backup Strategy and the Disaster Recovery Strategy?
- Is there a comprehensive Operational Support Model
- What are the provisions for Audit of data entry/changes and system access.

3.8 Stakeholders

3.8.1 Stakeholders

- Are all stakeholders, internal and external, clearly identified.
- Is there evidence of stakeholder communication with regards to functionality/impact/timings
- Are there plans to respond to technical support enquiries from external stakeholders if it is to be accessible to them e.g. online application process.

3.8.2 Requirements

- How did the project gather user requirements and maintain their input during the collation of the system specification?
- Have the requirements been gathered from the most appropriate people?
- Have decisions on requirements/functionality been left to ICT?
- Has the wider environment been considered during requirements gathering.
- Are all requirements clearly agreed and signed off.
- Are the requirements expressed in platform-independent terms? If not, what are the implications of locking in to a particular platform, particularly with respect to integration and data sharing?
- Are the requirements detailed in terms of an output-based specification or solution components? Has the implication of this choice been risk-assessed?
- Is all functionality clearly traceable to specific requirements and documented business needs.
- Is there a clear connection between Requirements and acceptance criteria.
- Is there sufficient control over Change.

3.9 Project closure/Transition

3.9.1 Testing

- Have the acceptance criteria for the system been written and agreed with the supplier and the Business/Users (or equivalent)?
- Has the live services organisation been fully consulted and are they a signatory to any acceptance signoffs?
- Is there clarity on acceptance criteria for every stage of testing?
- Is there a clear connection between acceptance criteria and Requirements
- Is the project manager actively managing the link between test acceptance and contract payment milestones?
- Are the planned tests representative of the live deployment or are there any significant differences between the development and live environments?
- Has network infrastructure been confirmed as suitable for new system deployment – e.g. network loadings, line speeds, server capacities etc and have these factors been taken into account when agreeing the test plans?

3.10 Lessons Learned

3.10.1 Active Learnings

- At project initiation, did the ICT lead seek out learnings from other projects, perhaps from a central Project Management Office (PMO) so as to inform initial planning?
- Is the ICT feeding into a Lessons Learnt log throughout the project, and actually recycling lessons into the next stage of the project, adjusting plans etc. accordingly?
- Does the project plan a Post Project Evaluation and does the organisation have a recipient for such learnings (e.g. a central PMO)?