
Document filename: ITK 2 0 Trust Operating Model Governance and Stakeholders v1.0.docx			
Directorate / Programme :	HSCIC - Architecture	Project	Interoperability
Document Reference :		HSCIC-ITK-ARCH-205	
Project Manager :	Rob Shaw	Status :	Final
Owner :	George Hope	Document Version :	1.0
Author :	George Hope	Version issue date :	23/06/2014

ITK Trust Operating Model Governance and Stakeholders

Document Management

Revision History

Version	Date	Summary of Changes
1.0	31/05/2014	First version issued by HSCIC

Reviewers

This document was reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
George Hope	ITK Architecture Lead	30/04/2014	1.0
Sanjay Paul	ITK Architect	30/04/2014	1.0
Richard Dobson	ITK Accreditation Manager	30/04/2014	1.0
David Barnet	ITK Communication and Messaging	30/04/2014	1.0
Nigel Saville	ITK Accreditation	30/04/2014	1.0

Approved by

This document was approved by the following people:

Name	Signature	Title	Date	Version
Shaun Fletcher		Head of Architecture	31/05/2014	1.0
Rob Shaw		Director Operational Services	31/05/2014	1.0

Reference Documents

Ref no	Doc Reference Number	Title	Version
1.			
2.			
3.			
4.			

Document Control:

The controlled copy of this document is maintained in the HSCIC corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

1	Introduction	4
1.1	Purpose of Document	4
1.2	TOM Documentation Set	4
1.3	Audience	4
1.4	Document Scope	5
1.5	Document Overview	5
2	Principles	6
3	Governance	7
3.1	Governance Structure	7
3.2	Governance Board	8
4	Example Stakeholder RACI	10
4.1	RACI Matrix	10
4.2	RACI Description	12

1 Introduction

This document forms part of the overall document set for the Interoperability Toolkit (ITK).

1.1 Purpose of Document

This document is part of the Trust Operating Model component of the Interoperability Toolkit. See the document “Trust Operating Model – Overview” for a more complete description of the document set.

This specific document provides guidance on the architecture-related aspects of Local Application Integration. It does this by providing a set of Architecture Principles to guide key design decisions in this space.

1.2 TOM Documentation Set

The position of this document in relation to the document set is shown below.

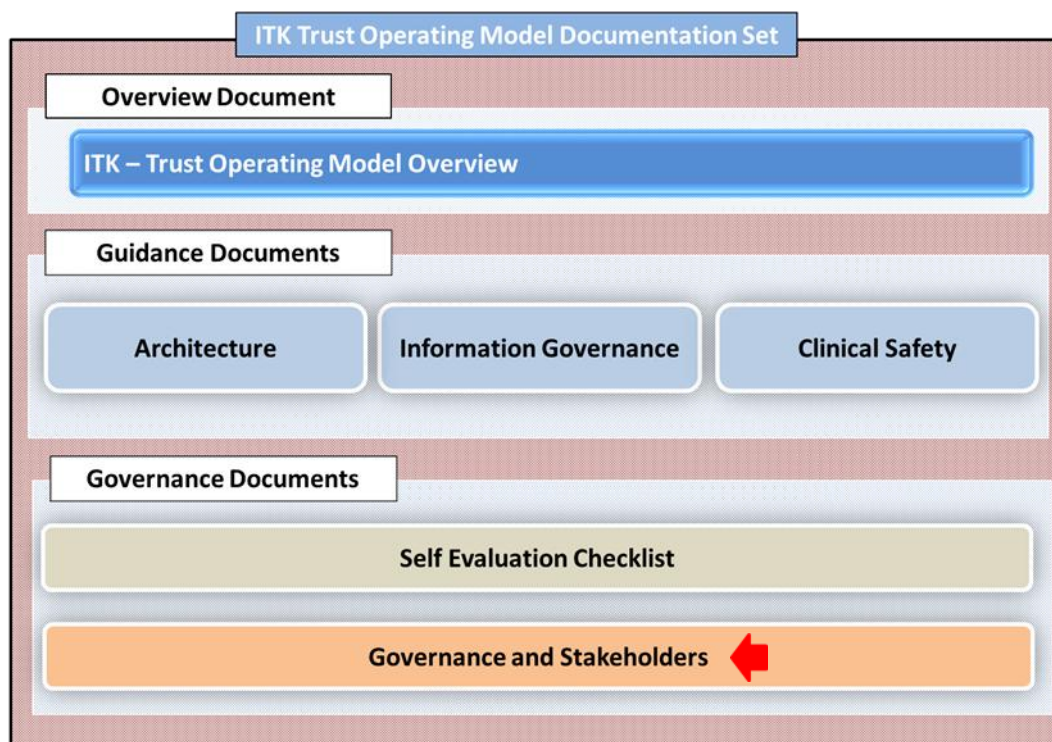


Figure 1 - The ITK Trust Operating Model Document Set

1.3 Audience

The primary audience for the Trust Operating Model is project teams within a Trust who are responsible for implementing a local integration project.

This document will be of particular relevance to project managers, and senior managers within a Trust who are responsible for signing off integration solutions.

Secondary audiences may include 3rd parties such as supplier and HSCIC architects

1.4 Document Scope

The Trust Operating Model focuses on integration between Local Trust Systems and Spine Compliant systems, and also on integration between Local Trust Systems and / or Non-NHS Systems within a Local Health Community environment. Please see the Overview document for further explanation of these concepts.

It does not cover integration at a National level through the Spine – existing Compliance documentation is already available on this topic.

Also note that the focus is on the key integration-specific aspects of a project. General topics necessary for any successful integration project (eg training, communications, service management etc) while important are not covered by this document.

1.5 Document Overview

The rest of this document covers the following topics:

- **Principles**
Underlying Principles which have shaped the approach
- **Governance**
Defines the governance structures and escalation routes for decision making and acceptance of risk.
- **Stakeholder RACI**
Shows examples typical stakeholder roles and responsibilities.

Toolkit Specifics

Note that this document provides generic architecture guidance that is relevant to any local integration solution.

However for projects making use of the Interoperability Toolkit, the Toolkit standards provide further explicit guidance and solutions. In addition the middleware provides pre-built services to assist. Boxes labelled “Toolkit Specifics” throughout the text highlight relevant points.

2 Principles

The following principles underlie the more detailed guidance given in the rest of this document:

Trust responsibility (from Overview)

A key principle applied to the governance model is that decisions regarding the exposure of data and services should be taken by those responsible for the data and services within the domain(s) being integrated.

Risk-based approach (from Overview)

The consultation taken and escalation paths required depend on an assessment of the level of risk involved.

Consideration of external implications (from Overview)

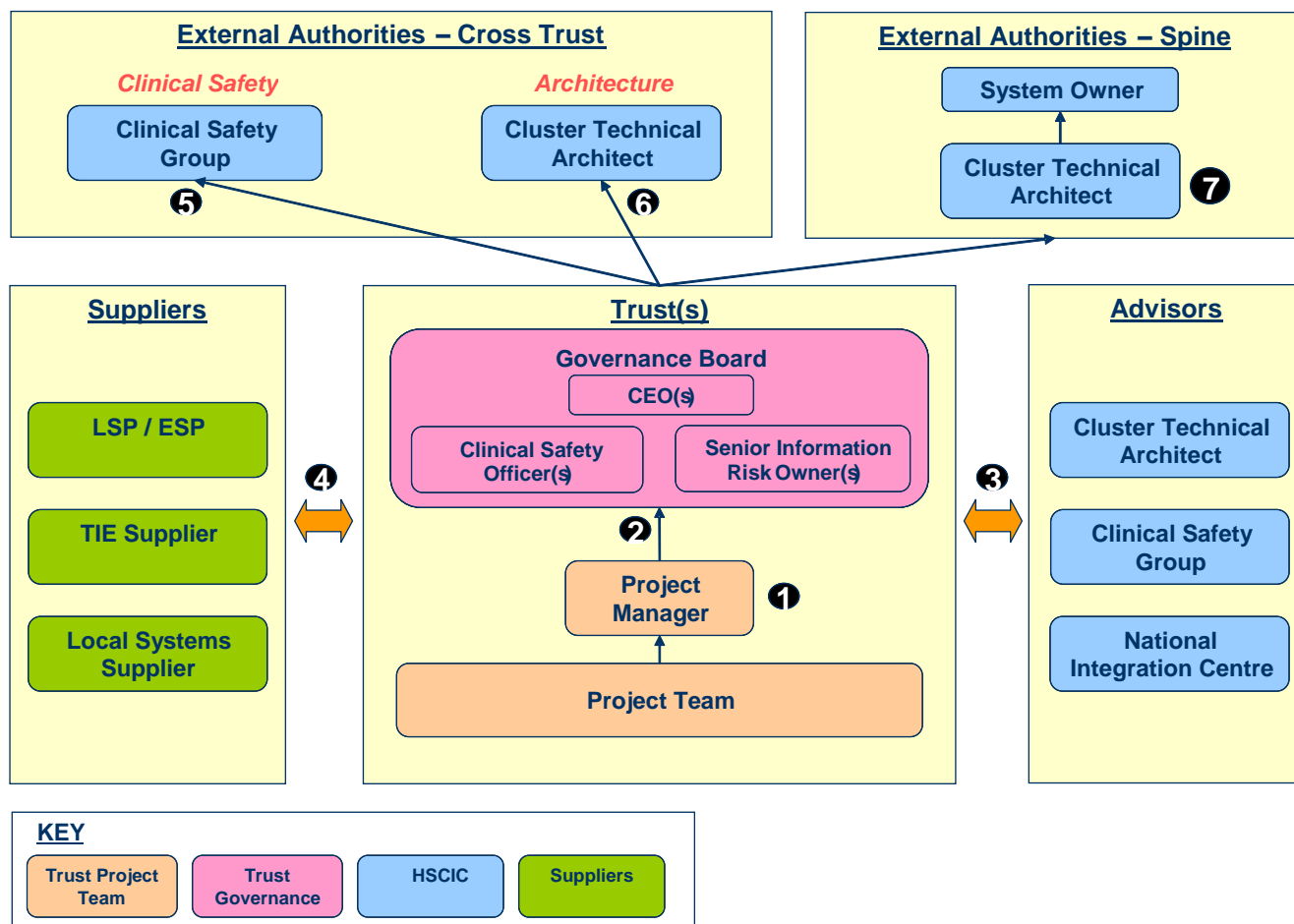
Escalation paths are explicitly defined in order to highlight the external bodies (whether other Trusts or HSCIC) who need to be consulted and/or provide sign-off.

3 Governance

3.1 Governance Structure

Inherent in the Trust Operating Model approach is the need for Governance structures to be defined. In particular there is a need for a decision making process to take the outputs of the Self Evaluation Checklist and make a Go / No-Go decision based on risk.

With this in mind, the diagram below shows the recommended Governance structures and escalation routes.



Key points are as follows:

1) Project Team and Project Manager

The integration project is run from within a Trust (or group of Trusts) by a Project Manager. The precise composition of this project team will vary depending on the individual project.

2) Governance Board

A Governance Board must be in place to approve key decisions and signoff the project implementation. The correct composition of this board is thus an essential factor, and is considered further in the next section.

3) Advisors

A number of expert advisors are available to assist the project team and Trust officers. These may provide validation and additional evidence to support the risk assessment work.

4) Suppliers

Suppliers will work together with the Trust Project team to implement the solution. Suppliers will also be able to provide expertise and advice, however ultimately the Trust(s) involved retain accountability for the assurance process.

5) Clinical Safety Risk Escalation - HSCIC Clinical Safety Group

In cases where it is deemed necessary, a Trust Clinical Safety Officer is responsible for escalating Clinical Safety related risks to the HSCIC Clinical Safety Group for a final decision. The precise circumstances are defined in the Clinical Safety Framework document, and relate to a high level of potential clinical risk (e.g. transformation of clinical data)

6) Architecture Risk Escalation - Cluster Technical Architect.

When systems beyond Trust boundaries are potentially impacted by the integration (eg performance), then the Trust is responsible for escalating Architecture related risks to the HSCIC Cluster Technical Architect for signoff.

7) Spine Risk Escalation – Cluster Technical Architect

When the Spine is potentially impacted by the integration then the Trust is responsible for escalating any Spine related risks to HSCIC Cluster Technical Architect. The CTA acts as a single point of contact into existing HSCIC governance structures, with responsibility for judging the level of escalation which is necessary based upon the nature of the risk. Ultimately this may involve escalating the matter to the defined System Owner (e.g. the HSCIC Program Director for the impacted Spine system).

3.2 Governance Board

As described above, a Governance Board must be in place to approve key decisions and signoff the project implementation. The composition of this Governance Board is thus of vital importance, and the characteristics required include:

3.2.1 CEO-level signoff authority

Ultimately the CEO is accountable for all activity (including integration projects) within a Trust. Thus, depending on the nature of the project, the CEO may sit on the Governance Board themselves, or may delegate responsibility to appropriate Trust officers.

3.2.2 Authority to accept all integration-related risks

These risks can be categorised as including:

- **Information Governance risks**

To accept these risks, representation will be required from the relevant Senior Information Risk Owner(s) (SIRO).

- **Clinical Safety risks**

This will require representation from the relevant Clinical Safety Officer(s).

- **Architecture risks**

This will require representation from Trust ICT management as well as, potentially, HSCIC Cluster Technical Architects and/or Supplier representatives

3.2.3 Authority to act on behalf of all affected organisations

All external implications of the project must be carefully considered, to ensure that all potentially impacted organisations are involved in the governance process. Examples of likely scenarios include:

- **Single Trust project**

If a project has no potential implications beyond a single initiating Trust, then the composition of the Governance Board will be relatively straightforward – consisting only of officers from the one affected Trust (e.g. SIRO, CSO, CEO)

- **Local Health Community project**

If a project involves joining up systems within a Local Health Community, then officers from all organisations within the LHC will need to be included in the governance process. (e.g. multiple SIROs and CSOs)

- **Project impacting shared LSP systems**

In a project impacting a shared system instance, then all organisations using the affected system instance must be involved in any decisions pertaining to acceptance of risk for that shared instance. Again, this may necessitate including multiple SIROs and CSOs in the project Governance Board¹.

¹ Note: If large numbers of Trusts are involved then it may clearly be time consuming to contact each external SIRO or CSO individually. Therefore it is anticipated that groups of Trusts may devise hierarchical structures to expedite this process. This might include, for example, the use of SHA-level officers, with the authority to speak on behalf of all Trusts in the CCG.

4 Example Stakeholder RACI

4.1 RACI Matrix

This section provides an example of a Stakeholder RACI. It summarises the stakeholders who may need to be involved, and their role (Responsible, Accountable) in each of the key activities outlined above. It is anticipated that Trusts will be able to use this as the basis for their own RACI grid, to be used for managing stakeholder engagement and governance activities when undertaking Trust integration projects.

The RACI itself is on the next page, and it is followed by a brief outline of the key points illustrated.

Note 1: The RACI shows only activities and stakeholders relating to the recommended governance processes. Additional items will clearly be needed for the project as a whole.

Note 2: For clarity the RACI shows only the Responsible and Accountable roles. There are other stakeholders who may need to Consulted or Informed at each stage, and examples are given in the text which follows.

Note 3: The RACI is intended as an example, to provide assistance to Trust project managers. It remains the project manager's responsibility to tailor this template for their own unique organisational and project circumstances.

	Trust Project Team			Trust Governance			Suppliers			HSCIC			
	Project Manager ³	System Users	Trust ICT Department	Clinical Safety Officer	Senior Information Risk Owner (SIRO)	Governance Board (on behalf of Trust CEO(s))	LSP / ESP	TIE Supplier	Local System Supplier ⁴	Cluster Technical Architects	Clinical Safety Group	CFH Change Management	NIC Non-Functional Test and Assurance Team
SPECIFICATION													
Document set overview and Self-Evaluation Checklist (1st Pass)	A / R												
Commercial - Volumetric Estimates (if necessary)	A		R										
Commercial - LSP Impact Assessment	A						R						
Commercial - TIE Licensing Assessment (if necessary)	A							R					
Information Governance - initial engagement	A / R												
Clinical Safety - initial engagement	A / R												
ARCHITECTURE AND DESIGN													
System Architecture definition			A / R				R	R	R				
End-to-End information flow mapping	A		R						R				
Self-Evaluation Checklist (2nd Pass)	A / R												
BUILD													
Interface Build							R	R	A / R				
TEST AND ASSURANCE													
System Testing	A	R	R						R				
Self-Evaluation Checklist (Final)	A / R												
Additional information on IG Controls (if necessary)	A								R				
Additional information on Clinical Safety (if necessary)	A			R					R				
Risk Assessment and Workoff Plan (if necessary)	A / R												
Signoff (IG)	R				R	A						R ¹	
Signoff (Clinical Safety)	R			R		A					R ²		
Final Signoff						A / R							
DEPLOYMENT													
Deployment	A / R						R	R	R				

1) IG Signoff by HSCIC Change Management only required if Spine may be impacted by risks introduced by the new interface

2) Clinical Safety Signoff by CSG only required if self-evaluation of clinical safety risk indicates that this is necessary

3) The "Project Manager" is a role. Depending on the project, it may or may not necessarily be performed by a full time resource with this job title

4) The "Local System Supplier" is a role. Not that it some Trusts this role may be performed by a development team within the Trust's own ICT department

4.2 RACI Description

4.2.1 Specification

- **Key Governance Activities**

An early first pass of the Self Evaluation Checklist is recommended - with the aim of both validating that all necessary aspects (both functional and non-functional) are covered by Requirements, and also identifying any potential problem areas for early stakeholder engagement. This may lead to a need for early initial engagement with IG and Clinical Safety experts.

Commercial implications should also be identified at this early stage, including any need for impact assessment by the LSP / ESP or impact assessment / licensing changes by TIE system suppliers. (Volumetric estimates may be needed to support this)

- **Key Stakeholders**

- Trust Project Manager – accountable for the process, and responsible for driving the Self Evaluation first pass and early engagement activities
- LSP / ESP and TIE suppliers – responsible for impact assessments, if required
- Trust ICT Department – responsible for volumetric estimates, if required

- **Other Potential Stakeholders**

- Trust Users, Managers, and Clinical Representatives – consultation on Volumetrics, IG, and Clinical Safety
- Trust Clinical Safety Offices, Caldicott Guardians, Senior Information Risk Officer, Legal Advisers – early expert consultation on IG and Clinical Safety

4.2.2 Architecture and Design

- **Key Governance Activities**

The key activity in this stage is the system Architecture definition, with this elaborating the technical details of the solution. An important additional part of this architecture work is developing an end-to-end information flow mapping – with this allowing the full implications of the proposed interface to be assessed. A second pass of the Self Evaluation Checklist should now allow all questions to be fully answered.

- **Key Stakeholders**

- Trust Project Manager – drives the process
- Trust ICT Department – Accountable and responsible for the overall system architecture definition. May need to work with the Local System supplier in mapping out the end-to-end information flows
- System supplier(s) – may be responsible for relevant aspects of the system architecture definition

- **Other Potential Stakeholders**

- Trust System Administrators – consultation on system architecture and design
- System Users – consultation on design of user-facing aspects
- Trust Clinical Safety Offices, Caldicott Guardians, Senior Information Risk Officer, Legal Advisers – further consultation for the second pass of the Self Evaluation Checklist
- LSP / ESP and TIE suppliers – consultation on the architecture, end-to-end information flows, and Self Evaluation Checklist
- HSCIC Expert Advisers – HSCIC experts such as Cluster Technical Architects and the Clinical Safety Group may be consulted about any areas of concern

4.2.3 Build

- **Key Governance Activities**

In the build phase the new interface is actually created. Progress should be tracked, and the risks and impact of any changes or deviations assessed.

- **Key Stakeholders**

- System supplier(s) – the supplier(s) of the new system are accountable and responsible for building the interface

- **Other Potential Stakeholders**

- Other suppliers and experts within the Trust may need to be involved as necessary

4.2.4 Test and Assurance

- **Key Governance Activities**

In addition to the normal functional tests, system testing should consider Volume and Performance testing (specifically checking for any impacts on existing Spine Compliant systems), and testing of messaging / interfacing issues such as sequencing, validation and concurrency.

An additional key assurance activity is then the finalisation of the Self Evaluation Checklist. This may include providing additional documentation about any IG or Clinical Safety implementation details which differ from previously established implementation patterns. Another possible outcome of the Self Evaluation Checklist may be the need to create a Risk Assessment and Workoff Plan to address any identified issues which are not immediately resolvable.

Formal signoff is then required, based on the Governance structures previously described.

- **Key Stakeholders**

- Trust Project Manager – responsible for driving the test and assurance process
- Trust Users and ICT Department – responsible for testing activities

- All suppliers – may need to be responsible for testing activities
 - SIRO and Clinical Safety Office – responsible and accountable for IG and Clinical Safety signoff. (The HSCIC Clinical Safety Group may also be responsible for signoff if the clinical safety risk is assessed as high)
 - Governance Board (on behalf of Trust CEO(s) – accountable and responsible for final signoff
- **Other Potential Stakeholders**
 - All of the stakeholders mentioned so far may need to be consulted in some form as part of finalising the Self Evaluation Checklist

4.2.5 Deployment

- **Key Governance Activities**

The system is deployed, including implementation of any process-based controls
- **Key Stakeholders**
 - Trust Project Manager – Accountable for the deployment
 - All Suppliers – may be responsible for different aspects of the deployment
- **Other Potential Stakeholders**
 - All of the stakeholders mentioned so far may need to be consulted in some form as part of dealing with any deployment issues

*** End of Document ***