



February 2025

Software Risk Management in GP Practices

Supporting practices to reduce the
risks for new software developments



Includes practical checklist

The Benefits of Getting This Right

Improving software compliance and compliance processes for GP practices.

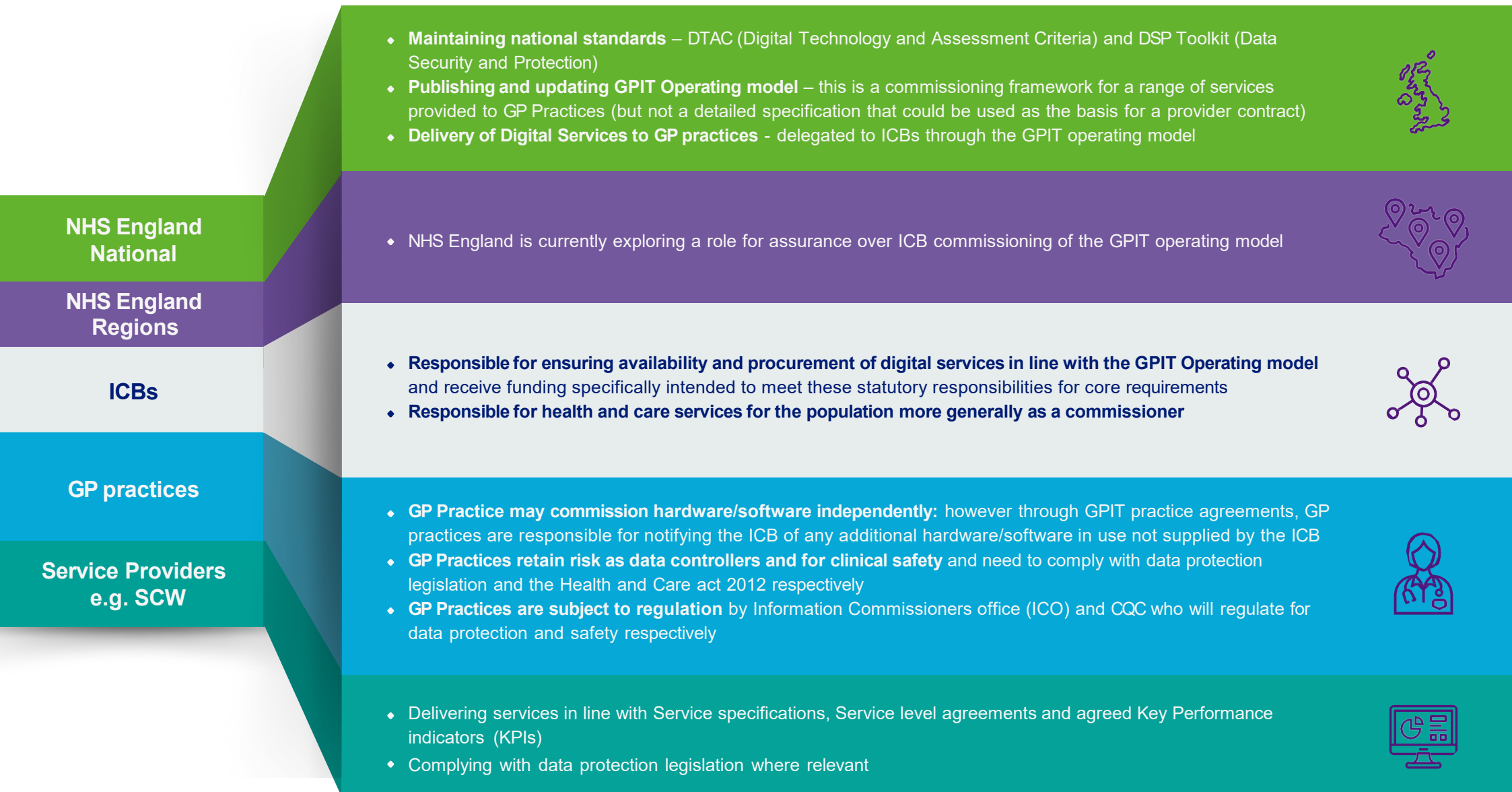
This pack has been developed to help support correct implementation of software and mitigate risks - for additional information [click here](#)

Included in this pack you will find a roles and responsibilities matrix, a process checklist and links to supporting documents.



Roles and Responsibilities

Defining team duties ensures accountability and prevents critical security or performance issues from being overlooked.



Accountability and Responsibility

Accountability and responsibility for different tasks is ambiguous. It is recommended that ICBs should clarify expectations locally (see example).

There are references to accountability and responsibility in national documentation, however, there is no single source of clarity on all tasks. We propose that this is necessary to tightly manage end to end software deployment. ICBs may make local decisions about service levels and therefore we recommend that ICBs review this and embed within local ICB-practice agreements.

A Accountable

R Responsible

RSP Responsible for managing service provider

- No accountability or responsibility

Service	Task (for a specific software deployment)	ICB led procurement		Practice led procurement	
		ICB	Practice	ICB	Practice
Information Governance	Commissioning of IG support service	A/R	-	A/R	-
	Creation/Sourcing of DPIA/DPA documentation	A/R	-	-	A/R
	Data Protection Officer (DPO) review of documentation	A/RSP	-	A/RSP	-
	Practice review sign off of documentation	A/R	A/R	-	A/R
Clinical Safety	Commissioning of Clinical assurance service	A/R	-	A/R	-
	Creation/sourcing of practice level DCB0160	A/R	-	-	A/R
	Clinical Safety Officer (CSO) review of documentation	A/RSP	A/R	-	A/R
	Practice review and sign-off of documentation	R	A/R	-	A/R
	Actioning practice level mitigations	-	A/R	-	A/R
IT	Commissioning of Core IG service	A/R	-	A/R	-
	Notifying ICB of intention to install new software in line with ICB – Practice agreement	-	-	-	A/R
	Notifying IT service of new software to commence cyber security and support level assessment	A/R	-	-	A/R
	Completion of cyber security and support level assessment	A/RSP	-	A/RSP	-
Contracting	Sourcing appropriate contract	A/R	-	-	A/R
	Review and sign off of contract	A/R	-	-	A/R

Service Baseline – GPIT Operating Model

ICB	CORE GPIT	GPIT services		Clinical safety Assurance	GPIT training
		DPO	IG		
BOB	SCW	SCW	SCW	Limited service*	SCW
Frimley: E&W Berks	SCW	SCW	SCW	Limited service*	SCW
Frimley: SH, NEHF	TTP	SCW	SCW	Limited service*	SCW
HIOW	TTP	AGEM	AGEM	Limited service*	AGEM
Kent & Medway	SCW	In-house	In-house	Limited service*	SCW
Surrey	SCW	In-house	SCW	Limited service*	SCW
Surrey	SCW	SCW	SCW	Limited service*	SCW

*GP practices who are independently procuring a software product may be required to buy in a Clinical safety assurance service if the ICB are not able to provide it. We recommend that before you start your journey you contact the ICB to better understand their offer.



Universal Information Governance Templates and FAQs



Data Protection Impact Assessment (DPIA)

A DPIA is a process that helps you systematically identify, analyse and where possible mitigate the data protection risks of specific projects, plans or activities within your organisation.

[Template DPIA
\(full version\)](#)

[Template DPIA
\(open access version\)](#)

[Watch video here](#)



Data Sharing agreement (DSA) & Data processing agreement (DPA)

A data sharing agreement is an agreement between two or more parties that outlines which data will be shared and how the data can be used. Not mandatory under UK GDPR rules, but best practice and helps address liability risks and concerns

A data processing agreement (DPA) is a contract between a data controller and a data processor that regulates any personal data processing conducted for business purposes. A DPA states the rights and obligations of each party concerning the protection of personal data, as required by Article 28 of the GDPR

**K&M IG team will provide both DSA
and DPA templates as required**



Privacy Notice (PN)

A PN is a document which informs people about how their data is being used, what their rights are under data protection legislation, and how they can exercise them.

[Template PN
\(full version\)](#)

[Template PN
\(open access version\)](#)

[Watch video here](#)

Regulations of AI and digital technology

The newly launched NHS **AI and Digital Regulations Service for health and social care** will help you learn what regulations to follow and how to evaluate effectiveness, whether you're a 'developer' of AI and digital technology or an 'adopter' who will buy or use them in health and social care.

The **regulations for adopters section** offer a platform where adopters can buy, deploy or use the technology in a health or social care setting to understand what regulations and best practice principles to follow when adopting your digital health technology.

You may also find useful the **Use of AI in evidence generation: NICE position statement**. This position statement provides clarity on how NICE will consider the use of AI methods in the generation and reporting of evidence to be evaluated within its guidance production programmes.

Software Deployment Process Practice Checklist - 1

We realise that this process may be overwhelming at times therefore, this checklist has been developed to help support you on your journey.

Important Guidance

- Ideally risk assessment and compliance is undertaken DURING purchase of a solution to ensure that a non-compliant solution is not purchased
- This checklist should be followed even where products are offered free of charge - it is always good practice to shop around as nothing is truly free in the long term, either charges will come once you are reliant on a product, or you may be paying for it with access to your patient data.
- The process to be followed is the same for the first installation of a new product, or installation of a product already in use. However, in the latter there will be example template documents e.g. DPIAs that can be used/modified - First installations will require more initial work to create documents and support services may have no prior knowledge of the product



Ensure you outline a requirement

Describe what you are trying to achieve in terms of product or service, what benefits you are looking to realise, how you would assess quality and desired balance between quality and price (e.g. 60/40 quality/price weighting).

12.5%
complete



Identify your procurement route - e.g. direct award or buying through a commercial framework. GP Practices often don't use commercial frameworks, but these usually give access to a template contract – the alternative is usually a contract written by a supplier which may not provide the same level of protection. Many frameworks charge a small amount for use, often cheaper than legal advice to review a contract or in the event something happens. To find available commercial frameworks, contact your ICB who will have knowledge and tools for this (you can also search yourself at find-tender.service.gov.uk).

25%
complete



Be mindful to longlist, shortlist and evaluate suppliers based on requirements

Not required if supplier has already been selected.

Develop longlisting to understand available suppliers. Shortlisting may involve eliminating based on pass/fail tests. Evaluation should assess quality and price. Make sure you check supplier accreditations.

37.5%
complete

Software Deployment Process Practice Checklist - 2

You are now ready to commence your commissioner's compliance risk assessment of preferred solution

These five processes should be **initiated** and **commenced** in **parallel**:

- ◆ Request **DTAC (Digital Technology Assessment Criteria)** from supplier - this contains several documents from the supplier which can be used across all other risk assessments
- ◆ **Information Governance Risk Assessment** (where relevant). Contact your local DPO (Data Protection Officer) for support, practices will need to find existing templates or write a **DPIA (Data Protection Impact Assessment)** and **DPA (Data Processing Agreement)** before signing these – **Information Governance Risk Assessment** is to ensure compliance with data protection laws, demonstrate that protection of individual's data has been considered and that a proportionate approach has been taken to mitigation of any risks
- ◆ **Clinical Safety Assessment** (where relevant). Contact your local Clinical Safety Assurance Officer (CSO) - practices will need to complete and sign **DCB0160 (Clinical Risk Management Standard) form**. If solution is medical device, need to ensure it has CE mark and registered with MHRA (Medicines & Healthcare Products Regulation Agency). **Clinical Safety Assessment** is a requirement of the Health and Social Care Act 2012 and ensures that services continue to be safe for patients which is regulated by the CQC
- ◆ IT provider risk assessment. Contact local IT service provider, as process will vary
- ◆ Seek permission from the ICB to install a solution following the locally agreed process as described in your GPIT Operating model practice agreement. Contact the GPIT lead at your ICB.

50%
complete

Software Deployment Process Practice Checklist - 3



	<p><u>Complete your purchase through signature of contracts</u> Inserting a break clause after 6 months is good practice and allows flexibility to exit a contract without financial penalty if not satisfied with product/service.</p>	<p>62.5% complete</p>
	<p><u>Ensure that your standing I G documentation is updated</u> Update ROPA (Record of Processing Activities) and Privacy notice (these are both elements of the Data Security & Protection toolkit which must be completed annually in any case).</p>	<p>75% complete</p>
	<p><u>Check support with deployment and implementation</u> You may be able to access support with this either from the supplier, the ICB or potentially through national support offers (if any).</p>	<p>87.5% complete</p>
	<p><u>Implement gold standard periodic reviews</u> Most of the compliance documents should contain a review date that should be diarised.</p>	<p>100% complete</p>

Supporting Documentation Checklist



Requirement:
Other

Helping you to track potential hazards, verify compliance, and maintain consistency throughout the project.


Document name	Purpose of document	What to do?	When required?
<u>DTAC</u> (<u>Digital Technology Assessment Criteria</u>) 	For a supplier to provide evidence of meeting clinical safety and IG (including cyber security) standards. This includes DCB0129 (a supplier assessment of clinical safety).	Request DTAC from supplier, send to IG, CSO, and IT	All Digital health technology
Local IT provider documentation e.g. CSU and ICB 	To help you understand: <ul style="list-style-type: none">• Implications for infrastructure: Compatibility/ burden/ cybersecurity risk (crossover with IG)• Any support requirements• Level of business continuity	Complete any elements needed by healthcare provider Pass documentation to supplier for any supplier elements.	All software

Supporting Documentation Checklist



Requirement:
Legal

Helping you to track potential hazards, verify compliance, and maintain consistency throughout the project.

Document name	Purpose of document	What to do?	When required?
<u>DCB0160</u> <u>Clinical Safety Standard</u> 	This supports the application of effective clinical risk management by healthcare provider organisations using the software (NHS England has started <u>a review of digital clinical standards DCB0129 and DCB0160</u> to ensure they remain up-to-date, practical and aligned with the latest advancements in healthcare technology and clinical practice.	Template document may already exist, ask supplier and Clinical Safety Officer (CSO) identifying hazards and risk mitigation considerations (at individual GP practice level).	Clinical solutions
Data Processing Impact Assessment (DPIA) - Controller to create 	This supports the controller (Practice) to demonstrate where data is to be processed, it has met the legal requirements applicable to the processing activity and has reduced risk as far as possible. Template document may already exist, ask supplier and Data Protection Officer (DPO).	Data controller should review and pass to DPO for review, then sign if agree with impact assessment. Ask the supplier for their DPIA to construct your own (it will contain the same information including e.g. how data is processed that you can then localise).	Data processing solutions

Supporting Documentation Checklist



**Requirement:
Legal**

Helping you to track potential hazards, verify compliance, and maintain consistency throughout the project.

Document name	Purpose of document	What to do?	When required?
Data Processing Agreement (DPA) If required (check with DPO if unsure) <input type="checkbox"/>	This supports defining a legally binding contract the arrangements between controller (Practice) and processor (supplier) for the processing of data and assurance to the controller that the processor is sufficiently competent to comply with the law.	Template document may already exist, ask supplier and DPO. Assuming this reflects the DPIA and this has been reviewed and signed, this document should then be signed by the data controller.	Data processing solutions
ROPA (Record of processing activities) and Privacy notice <input type="checkbox"/>	This will provide a clear record of all data processing by the organisation. This forms part of the Data Security and Protection (DSP) Toolkit that all organisations must complete annually.	Update ROPA and privacy notices to reflect change in data processing as required.	Data processing solutions