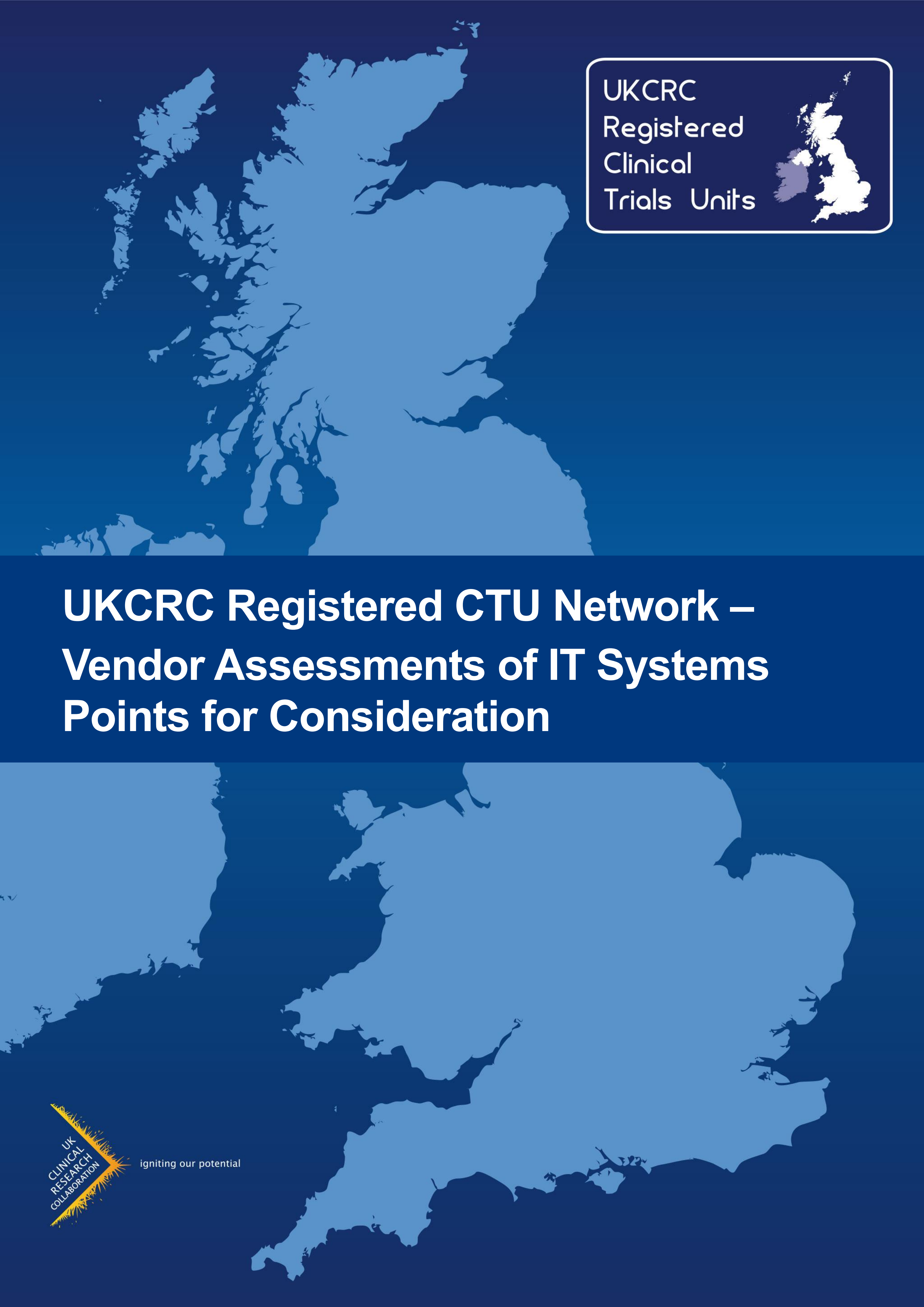

UKCRC Registered Clinical Trials Units

UKCRC Registered CTU Network – Vendor Assessments of IT Systems Points for Consideration

UK CLINICAL RESEARCH COLLABORATION

igniting our potential

Vendor Assessments of IT Systems
Points for Consideration

Contents

Purpose

The purpose of this document is to provide a framework for CTUs, to ensure all aspects are covered when assessing vendors for the provision/procurement of IT systems and services including compliance, user requirements and legal/contractual considerations.

Benefits of performing a vendor assessment are to ensure:

- compliance with European procurement directives and the UK regulations (https://www.gov.uk/guidance/transposing-eu-procurement-directives) if appropriate and legislative processes
- transparent, robust procurement and compliant procedures are followed (* see Table 2 Compliance)
- the solution is value for money; budgetary constraints are justifiable
- the solution is suitable and fit for purpose
- future road mapping and scalability are considered
- due diligence and ongoing assurance of service levels
- there is evidence of accountability

Scope

The scope of this document includes assessment of vendors for the provision of IT systems and services, including solutions that use cloud-based infrastructure.

This document is intended for use for software that will either be for collection of CTIMP and non-CTIMP data or used in conjunction with such systems and may therefore be modified / risk-adapted accordingly.

The content is not definitive and provides a suggested approach.

Procurement of hardware and associated peripherals is out of scope.

Introduction

It is the responsibility of the Sponsor (or delegated CTU) to ensure sub-contracted organisations that have been delegated trial tasks/responsibilities are following the appropriate regulatory and industry standards.

The following examples are not an exhaustive list of relevant standards

- GCP
- 21 CFR part 11
- GDPR
- ICT Security Standards (ISO27001)

The assessment helps to ensure that the vendor is compliant with all relevant regulations.

The framework also provides a means of assessing ongoing suitability of the vendor.

Table 1: Activities to consider when planning a vendor assessment

Prior to the Vendor Assessment	Activities to consider
Timing of Assessment	• Non-Disclosure Agreements / Confidentiality Agreements in place before assessment • Vendor assessment(s) should take place before vendor contract engagement and conclude before contract approval • Agree timely on-going assessments at intervals during the length of the contract
Vendor Assessment Team	• Identify key stakeholders • Expertise input/ representation from: o Information Security/ ICT o Data Management o Trial Management o Quality Assurance o Information Governance (Data Protection) o Procurement /Legal /Finance o Project Administrator o Representative(s) from vendor for clarifications
Meeting organisation	• Diary management /Timings • Time zones • Location(s) • Technology • Secure environment • Access • Practicalities i.e. rest breaks, lunch • 2–4 days per assessment, remote or on site
Documentation	• Pre-assessment questionnaire • If documents recently provided, to avoid duplication, confirm they are latest versions • Agenda, minutes and Assessment Tool document (if available) • SLA, Contracts, MSA, previous assessments / findings, • Training Record and CVs (vendor personnel) • Certificates / Qualifications i.e. ISO27001, DPIA (evidence to avoid extensive validation at a later point) • Current Client References – clarify service level, problems, implementation • Training documentation/user guides • Examples of IQ/OQ and SOPS • Third party agreements, sub-contractors • Previous assessments (including third party agreements) – serious findings and CAPA(s) • Vendor response, CAPA
Type of hosting	• Considerations for on-premise, cloud hosting, SaaS, PaaS etc.

Table 2: Compliance, System Considerations, User Requirements, Support, Contractual / Legal, Ongoing Management of contract

Compliance *	
Regulatory Framework	• GDPR • GCP • ISO27001 • Cyber Essentials • Data Security & Protection (DSP) toolkit
GDPR Compliance	• DPIA • Brexit considerations • Hosting location (UK/BREXIT) • Procedures on handling Data Breaches, who has access to data, type of data, where and how is data moved, stored
MHRA	• Procedures to support potential GCP Serious Breaches
Business Continuity	• Disaster Recovery and Business Continuity SOPs aligned with service
eConsent and eSignature	• MHRA guidance (https://www.gov.uk/government/news/improving-how-we-collect-and-document-consent)
Accessibility WCAG 2.1 Compliance – EU Legislation	• Vendor to provide an accessibility statement • Commitment to ongoing review and update according to EU legislation • Any considerations with respect to the product for accessibility
System Considerations Note that some of these items may be mandatory depending on the type of system under consideration	
Data	• Encryption in transit and at rest • GDPR measures to protect the data i.e. authorised access, provisions to prevent unauthorised access • Consider if this needs to be detailed in the PIS, adherence to data retention policy (if necessary) • Ability to retrieve data if any provider ceases to trade
User Interface	• Browsers used and supported • Operating systems used
Data Integration	• How to access data • API Integration requirements
Audit Trail	• Audit trail of in-system changes • monitoring in real time
Application lifecycle	• Product roadmap • Upgrade cycle and management (planned and unplanned) including communication and frequency • Deferring a patch or release

	• Processes to support change, release, and configuration management • Non-production environment • Clones of production • Levels of security on clones • Clone lifecycle, retention duration and destruction method (evidence of destruction if required) • Mid-study update procedures
Support	• Compensation for downtime, if contract terminated or hardware replaced are data securely deleted • SLAs (GDPR clauses need to be included or in separate agreements i.e. covering data processing activities, and where applicable, international transfers)
Hosting Approach	• On premise or Cloud hosting • Location and details of host • Security availability and integrity considerations • Procedures and audit trail to control access • Where multi-tenancy hosting approach is used, how is client isolation achieved • What Transparency Information (if any) needs to be disseminated to data subjects • International data flows (consider location of server) – i.e. will data be transferred for processing out of EU (or out of UK after end of the BREXIT Transition Period (31/12/2020) [1]
Performance	• Running of intensive activities impact on performance • Average response time expected
Availability	• Availability percentage achieved, and hours measured (consider core business hours) • Upgrades and other system maintenance scheduling • Can vendor provide an end monitoring tool to confirm system availability against product
Security of Application	• Penetration testing performed and by independent third party • Testing cycle and date recently tested • Timescales for recommendations implemented
Backup and Recovery	• Recovery procedure regularly tested, recovery objectives in a disaster scenario • Audit trail included in back up regimes and continues to function during restoration, *if applicable*
DNS Name	• can product use <*service*>.*HE*.ac.uk DNS name • is an IP address or an 'A Name' record provided • how are server certificates managed (assume SSL certificates are handled by HE institute)
Email	• Encryption • Can the product send emails and if so, using *HE* email address (i.e. HE.ac.uk) • Can emails be scheduled to automatically send

Authentication	• How is automatic 'User and Security Group Management' performed • Session timeout and force reauthentication • Single Sign On (SSO) and what type is used • 2-factor authentication (2FA)
Optional Services	• Does the product need to access HE data either hosted locally or another SaaS service, and how • Need to use data warehousing for reporting or analytics perform inbound and outbound SMS delivery • Require any HE provided encryption keys
User Requirements	
Requirements	• Functional and non-functional requirements – input from key stakeholders
Support, Ongoing Management of contracts, Contractual/Legal	
Key Documents	• Contract or agreement • Pricing • SLAs – to include handling of Breaches (e.g. Serious Beaches of GCP or Data Breaches) • Master Service Agreement • Data Processing Agreement • Agreements for international data flows, e.g. SCCs where applicable
Road maps	• Strategic Direction • Ongoing software innovation roadmap
Procedures	• To deal with: • Communication Plan between vendor and client • Procedure in place for effective and timely communication with client regarding Serious Data (DCO) and GCP breaches (MHRA) that support reporting timelines to Regulatory Authorities (RA) • Problems identified in software and updates regarding problems and mitigation plan

[1] **Data Protection NOTES –**

It is recommended to consult your organisation's Data Protection Officer for further advice on data protection regulatory requirements. The below information on Transparency Information, international dataflows and Data Controllership is given as a pointer only and reflects the requirements of the DPA 2018 / GDPR.

Transparency Information will need to be disseminated to data subjects where their Personal Data is processed. This could be done via addition to a participant Information Sheet for example. Transparency Information should include the minimum information required under applicable legislation (e.g. UK Data Protection Act 2018 / GDPR).

If data flows internationally for processing, the following will need to be in place:

- an Adequacy Decision (at the country-level), or
- alternative data protection legal pathway (at organisation level)

Adequacy Decisions may be “full” or “partial” (e.g. organisations subject to PIPEDA regulations in Canada).

Examples of alternative legal pathways are specific contracts e.g. Standard Contractual Clauses (SCC), Binding Corporate Rules.

Up-to-date information and guidance can be accessed via the ICO website: https://ico.org.uk/

Usually the Sponsor of a clinical trial is the Data Controller (DC) acting alone or in a joint capacity with other organisations: e.g. where the trial involves a collaborating Clinical Trials Unit (CTU) the host institution would also be a DC. Where the vendor is processing data on behalf of the DC(s), they act as Data Processor and a legal contract detailing the data processing activities must be agreed between the Data Processor and DC(s). The Data Processor must not sub-contract data processing activities to a third party without the prior written agreement of the DC. Where a trial involves multiple DCs the suitability of the Data Processor (and any third-party processors) should be agreed by all DC organisations.

Glossary

A Name	The A record maps a name to one or more IP addresses when the IP are known and stable.
BREXIT	***Brexit*** is the withdrawal of the United Kingdom (UK) from the European Union (EU)
Standard Contractual clauses (SCC)	Standard Contractual Clauses (**SCCs**) are standard sets of contractual terms and conditions that the sender and the receiver of the personal data both sign up to. They include contractual obligations that help to protect personal data when it leaves the EEA and the protection of GDPR.
Cyber Essentials	**Cyber Essentials** is a Government-backed and industry-supported scheme that helps businesses protect themselves against the growing threat of cyberattacks and provides a clear statement of the basic controls organisations should have in place to protect them.
DSP toolkit	The Data Security and Protection Toolkit (**DSP toolkit**) is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.
DPIA	A Data Protection Impact Assessment (**DPIA**) is a process to help organisations identify and minimise the data protection risks of a project. Organisations must do a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing.
GCP	*Good Clinical Practice* (***GCP***) is the international ethical, scientific, and practical standard to which all clinical research is conducted.
General data protection regulation (GDPR)	General data protection regulation (**GDPR**) https://gdpr-info.eu/
HE	Higher Education
ICO	The Information Commissioner's Office (**ICO**) is the UK's independent body set up to uphold information rights
IQ and OQ	**Installation qualification** (**IQ)** is a documented verification process that the instrument or piece of equipment has been properly delivered, installed, and configured according to standards set by the manufacturer or by an approved **installation** checklist. **Operational qualification (OQ)** is: Establishing confidence that process equipment and sub-systems are capable of consistently operating within stated limits and tolerances.

ISO27001	ISO/IEC 27001:2013 (also known as **ISO27001**) is the international standard that sets out the specification for an information security management system (ISMS). Its best-practice approach helps organisations manage their information security by addressing people and processes as well as technology
Master Service Agreement	A **master service agreement**, sometimes known as a framework agreement, is a contract reached between parties, in which the parties agree to most of the terms that will govern future transactions or future agreements
MHRA	The **Medicines and Healthcare products Regulatory Agency** (**MHRA**) is an executive agency of the Department of Health and Social Care in the United Kingdom which is responsible for ensuring that medicines and medical devices work and are acceptably safe.
PIPEDA	The **Personal Information Protection and Electronic Documents Act (CANADA)**
RFI	A ***request for information*** (***RFI***) is a common business process whose purpose is to collect written information about the capabilities of various suppliers.
RFP	A **request for proposal** (**RFP**) is a document that solicits proposal, often made through a bidding process, by an agency or company interested in procurement of a commodity, service, or valuable asset, to potential suppliers to submit business proposals.
Single sign-on	**Single sign-on** (**SSO**) enables users to securely authenticate with multiple applications and websites by logging in only once—with just one set of credentials (username and password).
SLA	A **service-level agreement** (SLA) is a **contract** that establishes a set of deliverables that one party has agreed to provide another. This **agreement** can exist between a business and its customers, or one department that delivers a recurring **service** to another department within that business
Two-factor authentication (2FA)	Two-factor authentication (**2FA**) is a security process in which users provide two different authentication factors to verify themselves. (e.g. a username and password and a randomly generated security code or text message code)
WCAG	Web Content Accessibility Guidelines (**WCAG**) is developed through the W3C process in cooperation with individuals and organizations around the world, with a goal of providing a single shared standard for web content accessibility that meets the needs of individuals, organizations, and governments internationally.

Acknowledgements:

Amanda Bravery – Head of ICT, Imperial Clinical Trials Unit (ICTU), Imperial College

Gavin Bravery – Enterprise-Wide Solutions Architect, Imperial College

Claire Johnson – Head of Quality Assurance and Regulatory Affairs, Centre for Trials Research, Cardiff University

Sharon Keen – Glasgow Clinical Trials Unit, University of Glasgow

Carolyn McNamara – Clinical Trials IT Manager, Clinical Trials and Statistics Unit, Institute of Cancer Research (ICR-CTSU)

Katie Neville – Quality Assurance Manager, Liverpool Clinical Trials Centre, University of Liverpool

-