Due diligence checklist: Cyber Essentials

Cyber Essentials and Cyber Essentials Plus (NCSC). NCSC, the United Kingdom.

Regime	Cyber Essentials
Regulator	NCSC
Country	the United Kingdom
Regulator's page	https://www.ncsc.gov.uk/cyberessentials/overview
Prepared	9 November 2026
Current version	https://www.vederca.com/market-scan/due-diligence/gb-cyber-essentials

What it is

A baseline many UK institutions ask suppliers to hold, with Plus adding an independent technical audit.

Who it applies to

Applies to every financial institution in the United Kingdom. A standard rather than a regulation: institutions ask for it, no regulator requires it of every vendor.

What to ask a vendor, and the evidence to request

#	Ask the vendor for	Evidence to request	Received
1	A current Cyber Essentials or Cyber Essentials Plus certificate	The current report or certificate, dated within the last twelve months, with its scope checked against the service being bought.	

In every case

- A named contact at the vendor responsible for this regime, and how the vendor tracks changes to it.
- Which named customers the vendor already serves under this regime, as references you may call.

This checklist is a starting point for a procurement team, not legal advice. Read it with the regulator's own page, your institution's policies and your legal and risk teams; the regime may have changed since the date on this document.