CLOUDSWITCHED

FREE RESOURCE — CERTIFICATION COMPARISON

Cyber Essentials vs ISO 27001

Two of the UK's most important security certifications, side by side. A clear, finance-and-board-defensible breakdown of scope, cost, timeline and recognition — with an industry-specific decision matrix to pick the right one for your business today, and a pathway for layering both as you grow.

CE+	ISO	8	SME
UK GOVT-BACKED TECHNICAL BASELINE	INTERNATIONAL ISMS STANDARD	DECISION SECTIONS HEAD-TO-HEAD	DECISION MATRIX FOR UK BUSINESSES

CYBER ESSENTIALS · ISO 27001 · UK SME · DECISION MATRIX

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Reference PDF

00

Why this comparison matters

UK organisations face a growing need to **demonstrate cybersecurity credentials** — whether to win government contracts, satisfy enterprise client requirements, qualify for cyber insurance or simply protect their own data. Two certifications dominate the conversation: **Cyber Essentials** (and its audited variant, **Cyber Essentials Plus**), and **ISO 27001**. Both improve security; they differ significantly in scope, cost, complexity and audience.

This guide is the deciding line in plain English. We compare scope, cost, timeline, recognition and renewal, walk through an industry-by-industry decision matrix, show how CE controls map directly to ISO 27001:2022 Annex A, and finish with a side-by-side pros-and-cons table you can take to your board. The answer for most UK SMEs is not “one or the other” — it is a sequence.

WHAT THIS GUIDE COVERS

Eight sections — **Overview & scope**, **Decision framework**, **Cost & resource**, **Industry requirements**, **CE □ ISO pathway**, **Certification process**, **Pros & cons** and a **Quick-reference decision matrix** — followed by an FAQ. Read-only reference document — no fillable form fields.

COMMON MISCONCEPTION — ISO 27001 DOES NOT INCLUDE CYBER ESSENTIALS

Many organisations assume that achieving ISO 27001 automatically covers Cyber Essentials. **This is not the case.** They are separate certification schemes with different assessment bodies, audit criteria and renewal cycles. You must apply for and pass each certification independently — even though there is significant overlap in the underlying technical controls.

The eight sections at a glance

- **01 The two schemes — overview & side-by-side.** What each certification actually is, plus a seven-criterion comparison table.
- **02 Decision framework.** Five questions that point to CE, ISO or both, and the order to do them in.
- **03 Cost & resource comparison.** Real UK pricing for SMEs, including the invisible internal cost lines.
- **04 Industry requirements.** Eight sectors and the certification each typically expects.
- **05 The CE □ ISO pathway.** How CE controls map directly to ISO 27001:2022 Annex A.
- **06 Certification process.** Step-by-step process for each, with timelines and stakeholders.
- **07 Pros & cons summary.** Strengths and limitations of each, table form.
- **08 Decision matrix & FAQ.** Pick the right starting point for your situation, plus the questions buyers most often ask.

01

The two schemes, side by side

One is a **technical baseline**; the other is a **management framework**. They are not competitors. They are complementary — and the simplest way to see why is to read them in parallel.

Cyber Essentials

A **UK Government-backed certification scheme** overseen by the NCSC and the IASME Consortium. Focused on five specific technical controls that protect against the most common internet-based cyber attacks.

- Two levels: **CE** (self-assessment) and **CE+** (independent technical audit).
- Five technical controls: **firewalls, secure configuration, security update management, user access control, malware protection**.
- Designed to be accessible for SMEs — lean process, prescriptive requirements.
- Required for many UK Government, NHS and defence supply-chain contracts.
- Annual certification with a full reassessment every 12 months.

ISO 27001

An **international standard** for Information Security Management Systems (ISMS), published by ISO/IEC. Covers people, process and technology across the whole organisation, on a risk-based footing.

- Full ISMS covering **governance, risk, people, process and technology**.
- **93 controls** across 4 categories in Annex A (2022 revision).
- Risk-based approach — controls applied where assessed risk justifies them.
- Internationally recognised across industries and geographies.
- **3-year certification cycle** with annual surveillance audits and recertification at year 3.

KEY TAKEAWAY

Cyber Essentials is a **technical baseline** — it ensures your systems are configured securely against common threats. ISO 27001 is a **management framework** — it ensures your entire organisation manages information security risks systematically. They cover different ground and are best used together.

01

Side-by-side criteria table

The seven decision criteria that matter most when picking a certification path — scope, cost, timeline, complexity, renewal, recognition and focus. Read both columns row by row; the differences become very concrete.

CRITERION	CYBER ESSENTIALS & CE+	ISO 27001
Scope	5 technical controls focused on internet-based threats	Full ISMS covering all information security risks
Cost	**£300 – £3,000** depending on size and CE vs CE+	**£10,000 – £50,000+** consultancy, implementation & audit
Timeline	**2 – 12 weeks** from start to certificate	**6 – 18 months** for initial implementation & certification
Complexity	**Moderate** — primarily technical controls	**High** — policies, risk assessments, management commitment, internal audits
Renewal	**Annual** — full reassessment every 12 months	**3-year cycle** — initial cert + annual surveillance + recert at year 3
Recognition	**UK Government**, NHS, defence supply chain	**International** — recognised globally across industries
Focus	Technical controls — *what is configured on your systems*	Entire information security management — *governance, risk, people and technology*

READ BOTH COLUMNS TOGETHER

The two schemes are **not in direct competition**. CE is fast, cheap and narrow; ISO is slow, expensive and broad. The hardest commercial mistake is treating them as an either/or — for any organisation that does both UK Government work and enterprise / international sales, the answer almost always involves both. The order in which you do them is the real decision (see Section 05).

02

Decision framework — which one do you need?

Five questions that point to the right starting point for your organisation. Answer them in order — the first “yes” is usually the one that decides the certification.

Q1 Do you bid for UK Government contracts?	**Yes** → you need CYBER ESSENTIALS at minimum. Many contracts mandate CE+ specifically. This is often a hard prerequisite before you can even bid — without it you are excluded at the gate.
Q2 Do you handle sensitive international data or serve global clients?	**Yes** → you need ISO 27001. International clients and partners typically expect ISO 27001 as the benchmark for information-security maturity. CE has limited recognition outside the UK and rarely satisfies an international procurement team.
Q3 Are you a startup or SME wanting a baseline quickly?	**Yes** → start with CYBER ESSENTIALS. Faster, more affordable, and a solid technical foundation. Build towards ISO 27001 later as you grow into enterprise sales.
Q4 Do you need to demonstrate mature security to enterprise clients?	**Yes** → pursue ISO 27001. Enterprise procurement teams — particularly in financial services, technology and healthcare — increasingly require ISO 27001 (or SOC 2) as a supplier condition.
Q5 Can you pursue both certifications together?	**Absolutely.** CE + ISO 27001 is a powerful combination. CE provides the technical baseline and satisfies UK Government requirements; ISO 27001 demonstrates comprehensive management to international clients. CE is an **excellent stepping stone** to ISO 27001.

WATCH OUT — THE RECOGNITION ASSUMPTION

UK-only assumptions break down quickly the moment a customer’s parent company is overseas. A US, European or Asian procurement team will typically not recognise **Cyber Essentials** as a security benchmark — they want **ISO 27001** or **SOC 2**. If any of your clients have a foreign HQ, factor ISO 27001 into your roadmap regardless of where you are based.

03

Cost & resource comparison

The true investment in each certification path — including the internal-resource and tooling lines most calculators forget. Figures are typical UK SME ranges (under 50 staff); enterprise scope multiplies both columns.

COST COMPONENT	CYBER ESSENTIALS & CE+	ISO 27001
Certification fee	£300 – £600 (CE self-assessment)	£5,000 – £15,000 (Stage 1 + Stage 2 audit)
Assessment / audit	£1,500 – £3,000 (CE+ technical audit)	£3,000 – £8,000 / year (surveillance audits)
Consultancy support	£1,000 – £5,000 (optional, recommended)	£10,000 – £30,000 (implementation support)
Internal resource	1–2 people, part-time for 2–12 weeks	Dedicated project lead for 6–18 months
Ongoing maintenance	Annual reassessment preparation	Continuous ISMS management, internal audits, surveillance
Tooling	Vulnerability scanner (often included)	GRC platform, risk register, document management
Total Year 1 (typical SME)	**£1,500 – £5,000**	**£15,000 – £50,000+**

BUDGET REALITY CHECK

For SMEs with fewer than 50 employees, **Cyber Essentials Plus typically costs £2,000–£5,000 all-in** with consultancy support. **ISO 27001 for the same organisation lands at £15,000–£30,000 in the first year**. Factor in ongoing maintenance when budgeting — ISO 27001 requires continuous effort, not a one-off project. Plan for a steady-state ISMS spend of **£5,000–£15,000 / year** after Year 1.

DON'T CHOOSE BASED ON COST ALONE

The right certification depends on your **business objectives, client requirements and growth plans** — not just budget. A **£2,000 CE+ certificate** that unlocks a **£500,000 government contract** is far better value than saving money by doing nothing. Equally, investing **£25,000 in ISO 27001** can unlock enterprise clients worth millions in recurring revenue. Treat both as commercial investments, not compliance overheads.

04

Industry-specific requirements

Different sectors expect different things. Eight UK industries below; the “CE” column reflects what is needed to bid, and the “ISO” column reflects what enterprise customers in the sector typically expect.

INDUSTRY	CYBER ESSENTIALS	ISO 27001	NOTES
Public Sector	REQUIRED	OPTIONAL, VALUED	CE/CE+ mandatory for contracts involving personal or sensitive data. ISO 27001 increasingly expected for larger contracts.
NHS & Healthcare	REQUIRED	RECOMMENDED	CE required for DSPT (Data Security & Protection Toolkit) alignment. ISO 27001 expected for larger NHS suppliers and digital-health providers.
Financial Services	RECOMMENDED	OFTEN EXPECTED	FCA does not mandate either, but ISO 27001 is widely expected by banks and insurers from third-party suppliers. CE is a good baseline.
Legal	OFTEN REQUIRED	PREFERRED FOR LARGE FIRMS	Law Society and SRA encourage CE. Large law firms and those handling sensitive cases increasingly pursue ISO 27001.

PUBLIC SECTOR & REGULATED INDUSTRIES

The four sectors above all share a common pattern: **CE is the floor**, ISO 27001 is the ambition. The next page covers the four sectors where the answer is more nuanced — particularly tech, defence and education, where one buyer in the supply chain can shift the requirement entirely.

04

Industry requirements continued

The remaining four sectors — technology, construction, defence and education — where buyer-by-buyer variance is widest. Read the “Notes” column carefully: a single anchor customer can move you from “optional” to “mandatory” overnight.

INDUSTRY	CYBER ESSENTIALS	ISO 27001	NOTES
Technology / SaaS	RECOMMENDED	EXPECTED FOR ENTERPRISE	Enterprise clients almost universally expect ISO 27001 (or SOC 2) from SaaS providers. CE is a good starting point but rarely sufficient alone.
Construction	REQUIRED FOR GOVT	OPTIONAL	CE required for government subcontracts and increasingly expected on major infrastructure projects.
Defence	REQUIRED	OFTEN REQUIRED	Defence Cyber Protection Partnership (DCPP) mandates CE. Larger defence contracts often require ISO 27001 additionally.
Education	RECOMMENDED	OPTIONAL	DfE recommends CE for schools and academies. Universities handling research data may need ISO 27001 to host funded projects.

USE THIS AS A STARTING POINT, NOT THE FINAL WORD

Within every sector, individual procurement teams set their own bar. **Read the supplier-security clause** in any tender document before you decide which certification you need — the answer is sometimes in the small print, and the “recommended” default for the industry may have already moved to “required” for a specific buyer.

05

The CE □ ISO 27001 pathway

Cyber Essentials is an **excellent stepping stone** to ISO 27001. The five CE technical controls map directly to several ISO 27001:2022 Annex A controls. The additional work for ISO 27001 focuses on governance, risk management, documentation and the broader organisational processes that wrap those controls.

Control mapping — CE control □ ISO 27001:2022 Annex A

CE CONTROL	ISO 27001 ANNEX A MAPPING	ADDITIONAL ISO 27001 REQUIREMENTS
Firewalls	A.8.20 Network Security A.8.21 Security of Network Services	Network segmentation strategy, monitoring, documented network architecture.
Secure Configuration	A.8.9 Configuration Management A.8.19 Installation of Software	Baseline configuration standards, change management process, hardening guides.
Security Update Management	A.8.8 Management of Technical Vulnerabilities A.8.19 Installation of Software	Formal vulnerability management process, risk-rated patching, vulnerability scanning programme.
User Access Control	A.5.15 Access Control A.5.16 Identity Management A.8.2 Privileged Access Rights	Formal access control policy, identity lifecycle management, access reviews, segregation of duties.
Malware Protection	A.8.7 Protection Against Malware	Malware incident procedures, user awareness training, multiple defence layers documented.

HOW THE MAPPING HELPS

Every CE control you have implemented is **direct evidence** against the ISO 27001 Annex A control alongside it. Your CE+ technical assessment report becomes a re-usable artefact in the ISO 27001 internal audit cycle — particularly for A.5.15, A.5.16, A.8.2, A.8.7, A.8.8, A.8.9, A.8.19, A.8.20 and A.8.21. The work itself is not duplicated; the documentation effort wraps around it.

05

What ISO 27001 adds beyond CE

The 88 Annex A controls that don't map back to a CE control — and the management-system work that wraps them — split into the two themes that consume the most implementation time: governance & management, and operational controls.

Governance & management

- Information security policy framework
- Documented **risk assessment methodology**
- **Statement of Applicability** (SoA) for all 93 Annex A controls
- Management review and explicit top-management commitment
- **Internal audit programme**
- Continual improvement process

Operational controls

- Asset management and classification
- Supplier security management
- Business continuity & disaster recovery planning
- Physical security controls
- HR security — screening, training, leavers process
- Incident management procedures

THE SMART PATH

For most UK SMEs the recommended approach is staged: **(1)** achieve CYBER ESSENTIALS to establish the technical baseline; **(2)** progress to CE+ for independent verification and to meet government bidding rules; **(3)** use CE as the foundation for an ISO 27001 ISMS implementation. This spreads cost and effort, builds internal capability progressively, and satisfies UK Government requirements along the way.

06

Certification process — start to certificate

What each certification process actually involves, in order. CE+ is a short, prescriptive project led by IT. ISO 27001 is a multi-stage organisational programme that touches every department.

Cyber Essentials Plus process

01 Define scope — devices, users, networks in scope
02 Implement the 5 technical controls
03 Complete CE self-assessment questionnaire
04 Obtain CE certificate (foundation level)
05 Schedule CE+ technical assessment with assessor
06 Undergo hands-on audit (remote or on-site)
07 Remediate any findings within the assessor window
08 Receive CE+ certificate — valid 12 months

Timeline: 2–12 weeks · **People:** IT team + a senior responsible officer

ISO 27001 process

01 Gap analysis against ISO 27001 requirements
02 Define ISMS scope and organisational context
03 Risk assessment and risk treatment plan
04 Develop policies and procedures (ISMS docs)
05 Implement Annex A controls per Statement of Applicability
06 Staff training and awareness programme
07 Internal audit cycle
08 Management review meeting
09 Stage 1 audit — documentation review
10 Stage 2 audit — implementation review
11 Certificate issued — 3-year cycle, annual surveillance

Timeline: 6–18 months · **People:** all departments, top management, external certification body

WHERE THE TIME REALLY GOES

CE+ time is dominated by **technical remediation** — patching, MFA rollout, removing local admin rights, retiring unsupported software. Allow a **two-week buffer** for findings between the scan and the certificate.

ISO 27001 time is dominated by **documentation and risk-assessment work**, not technical controls. Most SMEs already have ~70% of the controls in place; the gap is writing them down, governing them and proving they run. Budget for the project lead to spend **2–3 days a week** on this from kickoff to Stage 2.

07

Pros & cons summary

Where each certification earns its keep — and where it falls short. Read both tables before committing to either path; the limitations often matter as much as the strengths.

CE / CE+ Strengths & limitations

STRENGTHS	LIMITATIONS
+ Fast to achieve — weeks, not months	- UK-focused — limited international recognition
+ Affordable for SMEs (£300–£3,000)	- Narrow scope — only the 5 technical controls
+ Directly addresses most common attack vectors	- Does not address governance, risk management or people
+ Mandatory for UK Government contracts	- Annual full reassessment (no surveillance model)
+ Clear, prescriptive requirements — low ambiguity	- May not satisfy enterprise client security questionnaires

ISO 27001 Strengths & limitations

STRENGTHS	LIMITATIONS
+ Internationally recognised and respected	- Expensive — £15,000–£50,000+ in Year 1
+ Comprehensive — covers all aspects of information security	- Time-intensive — 6–18 months to implement
+ Risk-based — tailored to your specific threats	- Requires ongoing management and dedicated resource
+ Satisfies most enterprise and international client requirements	- Documentation burden can be significant
+ 3-year cycle with annual surveillance — less disruptive	- Does not automatically satisfy UK Government CE requirements

OUR RECOMMENDATION FOR MOST UK SMES

Start with Cyber Essentials Plus. It provides immediate, tangible security improvements, satisfies UK Government bidding rules, and gives you a clean foundation for ISO 27001 when the time is right. If you are already selling to enterprise clients internationally — or plan to within 12 months — begin **ISO 27001 planning in parallel** so the gap-analysis is done before the first enterprise buyer asks for the certificate.

08

Quick-reference decision matrix

Eight common UK SME profiles and the certification that fits. Match the line that describes your business and pick the column on the right.

YOUR SITUATION	RECOMMENDATION	RATIONALE
Small business, limited budget, UK-focused clients	CE / CE+	Maximum security improvement for minimum investment. Meets UK requirements.
Bidding for UK Government or NHS contracts	CE+ (MANDATORY)	Non-negotiable requirement. Start immediately if you do not have it.
SaaS provider selling to enterprise clients	ISO 27001	Enterprise procurement teams require ISO 27001 (or SOC 2) as standard.
Growing company with UK and international clients	CE+ THEN ISO	CE+ for quick wins and UK compliance. ISO 27001 for international credibility.
Defence supply-chain participant	BOTH REQUIRED	CE+ mandated by DCPP. ISO 27001 expected for sensitive defence contracts.
Startup seeking first security credential	CE FIRST	Quick, affordable, demonstrates security commitment to investors and early clients.
Large organisation with existing security programme	ISO 27001	Formalises existing practices. CE+ can be added easily alongside ISO.
Regulated industry — finance, healthcare, legal	BOTH RECOMMENDED	CE+ for baseline compliance. ISO 27001 for regulatory alignment and client trust.

THE ORDER MATTERS

Where the matrix says **"both"**, the usual sequence is CE+ FIRST → ISO 27001 SECOND. CE+ gives you a 2–12 week win, removes the most common attack surface, and produces evidence the ISO 27001 audit team will accept directly against several Annex A controls — particularly A.8.7, A.8.8, A.8.20 and A.5.15.

09

Frequently asked questions

The questions buyers and finance directors ask most often when scoping a certification programme. Short answers; the rest of the guide has the long ones.

Does ISO 27001 include Cyber Essentials?

No. They are separate certifications with different assessment bodies and renewal cycles. An organisation already certified to ISO 27001 will, however, find CE+ *straightforward* to achieve — most of the underlying technical controls already overlap.

Can I get both certifications at the same time?

Yes. Many organisations pursue CE+ first (2–12 weeks) and then use it as the foundation for ISO 27001 (6–18 months). Some run both in parallel where there is enterprise client pressure.

Do I need a consultant?

For CE / CE+, consultancy is **optional but recommended** — the scope is small enough that an in-house IT lead can run it if they have the time. For ISO 27001, **external consultancy support is strongly recommended** for a first-time implementation; the documentation overhead is the single biggest reason in-house programmes stall.

How long do certifications last?

CE / CE+ are valid for **12 months** and require a full reassessment. ISO 27001 runs on a **3-year cycle** with annual surveillance audits and recertification at year 3.

What happens if I fail the assessment?

CE+ offers a **remediation window** — typically 30 days — to fix any findings and be retested without restarting. ISO 27001 may issue minor or major **non-conformities** that must be resolved before the certificate is granted; major non-conformities trigger a follow-up audit.

Is Cyber Essentials enough for GDPR compliance?

CE helps demonstrate the "appropriate technical measures" obligation under **UK GDPR Article 32**, but it does not cover all GDPR requirements — data mapping, DPIA, lawful basis, privacy notices, DSAR handling and breach reporting all sit outside its scope.

Not sure which certification to pursue?

Cloudswitched delivers both CE+ certification services and ISO 27001 consultancy support — in sequence or in parallel. We can help you choose the right path, then walk you through it.

cloudswitched.com

info@cloudswitched.com

CLOUDSWITCHED

CYBER SECURITY · COMPLIANCE · CLOUD

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom