CASE STUDY

How CBE Companies achieved ISO 27001 certification in record time.

How CBE and Protecht led a 12-week sprint to formalise information security governance, strengthen audit readiness, and build lasting client confidence.

protechtgroup.com

Summary

For more than 90 years, CBE Companies has operated in industries where trust is vital. As a provider of accounts receivable management and call centre solutions, based in Cedar Falls, Iowa, its clients expect not only operational reliability, but demonstrable discipline in how risk and security are governed.

That expectation became explicit when a major client required ISO 27001:2022 certification within a fixed and unusually compressed timeline – within 90 days rather than the typical 6-12 months.

CBE already operated with a strong information security posture aligned to NIST SP 800-53 good practices in support of a variety of government clients and other customers. What it did not yet have was auditable alignment with ISO 27001:2022.

Rather than assembling proof through disconnected tools or manual workarounds, CBE turned to Protecht, a platform it was already using to support its enterprise risk management program. What followed was a 12-week sprint that gave formal structure to the entire organisation's information security approach.

"Most companies take more than six months to get certified. We had 12 weeks – and we did it."

Nick Michael
Chief Risk Officer, CBE Companies

The challenge: from confidence to credibility

Client expectations around information security assurance have hardened. Self-attestation is no longer enough. For organisations like CBE, that shift creates pressure not only to operate securely, but to demonstrate that security in a way that stands up to scrutiny and external audit.

While CBE had invested heavily in information security practices aligned separately to recognised NIST, PCI, ISO and SOC 2 frameworks, several gaps became clear once formal certification with ISO 27001 entered the picture. There was no single information security management system tying risks, controls, policies, and evidence together. Audit activities existed, but not as documented, recurring processes. Relationships between different frameworks were understood conceptually but not mapped in a way an auditor could follow.

All of this had to be addressed before their critical client agreement could be finalised. A process that typically takes 6-12 months had to be completed within 12 weeks.

"We used to be able to say we were compliant. Now clients want the actual certification, and having been through it I understand why."

Nick Michael,
Chief Risk Officer, CBE Companies

Why CBE chose Protecht

CBE was not starting from zero. The organisation had already partnered with Protecht in 2023 to strengthen its enterprise risk management foundation. Over time, that implementation expanded to include vendor risk and contract management, with a deliberate focus on using a single platform rather than adding point solutions.

That decision was pivotal.

Protecht's risk-centric architecture meant existing controls and risk relationships could be extended, not rebuilt. The software's ability to map and manage multiple frameworks in parallel allowed CBE to avoid duplicating work at precisely the moment time was most constrained.

Just as importantly, CBE was looking for a partner, not just a software vendor. The relationship was characterised repeatedly as collaborative rather than transactional.

That partnership mindset became critical as timelines tightened.

Building discipline at speed

Working closely with CBE's security and risk leaders, Protecht helped stand up a complete information security management system (ISMS) in a matter of weeks. Controls were formalised and mapped across frameworks. Policies, risks, and evidence were consolidated into a single environment. More than 30 recurring audit processes (daily, weekly, monthly, and annual) were defined and embedded. Framework controls now feed directly into CBE's organisational risk strategy.

For teams accustomed to operating securely but informally, the shift was material.

The platform also enabled deeper asset-level traceability. Hardware, systems, and controls could be linked in a way that allowed evidence to be followed from policy to implementation. This level of granularity proved essential during the audit process.

"Why invent another tool when we already had so much in Protecht?"

Shawn Garrington,
Information Security Manager,
CBE Companies

Meeting and exceeding audit expectations

The certification process itself unfolded in two stages.

The first stage of the audit surfaced predictable pressure points. Processes that existed in practice needed to be formalised. Evidence had to be tightened and clearly linked to specific control requirements. Under a conventional timeline, these gaps would be addressed incrementally. Here, they had to be closed immediately.

Protecht worked closely with CBE to remediate findings, align documentation, and reinforce the links between risks, controls and supporting evidence. The platform made it possible to respond to auditor requests without fragmentation or rework, even as requirements became more granular.

By the second stage, the audit shifted from interrogation to validation. Controls could be traced through policies, assets and evidence. Governance processes were visible, repeatable and owned. What initially appeared ambitious proved defensible.

The result was not just a completed ISO 27001:2022 audit, but a demonstration of discipline that met – and in some respects exceeded – expectations for a first certification cycle.

Outcomes that extend beyond certification

While the immediate objective was time-bound, the outcome was structural.

CBE now operates with a documented, repeatable security governance model. Executive and board reporting is more consistent. Client information security assessments are handled with greater confidence, supported by clear evidence trails rather than narrative explanation.

The organisation is also positioned to scale. Controls that have been mapped once can now be reused across additional standards and client requirements without starting again. Future audit cycles are expected to require far less manual effort.

An insight CBE found as a result of the implementation was that ISO was more of a process audit versus a control audit, looking at processes from end to end and then identifying gaps or non-conformities to address.

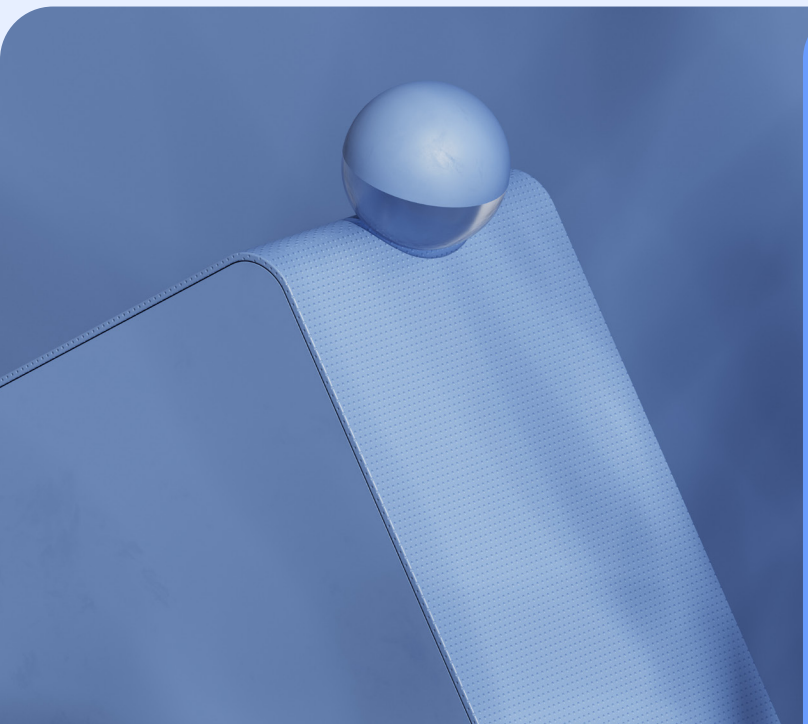
Overall, CBE found that the ISMS that Protecht implemented provides better visibility into audits for both the risk team and the executive team, since it integrates ISMS with the enterprise risk management system. This gives CBE's executives the confidence of a single, consistent position to understand and make decisions about where the risks are for the business.

A partnership that continues

Throughout the project, CBE emphasised that outcomes were driven as much by people as by technology. Protecht's collaborative approach, including responsiveness, judgement, and hands-on collaboration were keys to successfully delivering the project under pressure.

The partnership continues to grow as CBE expands its use of Protecht across ERM, ISMS, vendor and contract management, PCI DSS, and emerging capabilities like Cognita AI. Protecht remains a core strategic component of CBE's risk program and a key enabler of its future resilience. What began as a compressed compliance exercise became a lasting uplift in how security risk is governed and demonstrated.

If you are facing similar pressure to demonstrate security, accelerate certification, or unify fragmented frameworks, the right foundation makes all the difference.



"It felt like one team, not a vendor relationship."

Shawn Garrington,
Information Security Manager,
CBE Companies

Find out more

eBook

Explore how leading organisations are approaching modern cyber risk management in our cyber risk eBook.

Download now

Cyber solution

Learn more about how Protecht supports end-to-end cyber and IT risk management within a single platform.

Find out more

Demo

See it all in action by requesting a demo of Protecht's integrated GRC platform.

Request a demo

About CBE Companies

Founded in 1933, CBE Companies provides accounts receivable management services and global outsourced contact centre solutions. Headquartered in Cedar Falls, Iowa with more than 1,200 employees across four locations worldwide, CBE supports clients by connecting customers with resolution pathways while maintaining a focus on operational performance, customer experience and data security.

About Protecht

For over 25 years, Protecht has redefined the way people think about risk. We provide a complete solution of AI-enabled governance, risk and compliance software supported by training and advisory services to businesses, regulators, and governments across the world. Our Protecht SaaS GRC platform lets you manage your risks in one place: risk, compliance, incidents, KRIs, vendor risk, cyber and IT risk, operational resilience, business continuity, audit, and more.

Visit our website:
protechtgroup.com

Email us:
info@protechtgroup.com