CASE STUDY

Private Medical Organisation: Overhauling Third-Party Risk Management with OneTrust

Overview

The client is one of the leading independent healthcare providers in England, operating a large number of facilities across the country.

Its hospitals and clinics deliver a wide range of specialised clinical services, including routine and complex surgery, day case procedures, diagnostic services, and physiotherapy.

Given the breadth of services delivered and the critical role of its suppliers — from those providing clinical systems and medical equipment to contractors working within hospital sites — robust supplier assurance was essential to ensure patient safety, compliance, and operational resilience.

The Challenge

The organisation identified weaknesses in its supplier assurance process, which was inadequate for the scale and diversity of its operations. Existing processes were inconsistent, labour-intensive, and failed to provide meaningful assurance over third-party suppliers handling sensitive data and critical services.

The supply chain was vast and varied, from medical equipment providers supporting surgery, to on-site contractors, to software developers delivering critical healthcare applications. Any new framework had to be robust, flexible, and able to proportionately assessing different types of supplier risk.

Supplier assessments also needed to align to the Digital Technology Assessment Criteria (DTAC), which brings together requirements for clinical safety, data protection, technical security, interoperability, usability, and accessibility. The new assurance process also had to meet the relevant clauses of ISO 27001 relating to supplier relationships and third-party risk.

© 2025 i3Secure Ltd

Our Solution

i3Secure was engaged to redesign and deliver a new supplier assurance model. The engagement began with a discovery phase to understand the current process, identify risks, and map inefficiencies. This diagnostic stage provided the evidence base for change.

We then designed a new supplier assurance framework, supported by a policy, standard, and procedure document, to formalise governance and embed accountability across the organisation.

Crucially, the programme was delivered in close collaboration with the organisation's Procurement and IT departments, ensuring supplier assurance became an integrated part of purchasing, contracting, and technical risk management rather than a standalone compliance activity.

Key elements of the delivery included:

Supplier Onboarding & Triage: Introduced a risk-based triage system to categorise suppliers by impact, tailoring requirements appropriately (e.g., lighter requirements for low-risk contractors, enhanced due diligence for critical technology providers).

Process Redesign & Governance: Standardised workflows for onboarding, due diligence, and ongoing monitoring, supported by governance documentation aligned to ISO 27001 supplier relationship clauses and DTAC requirements.

Technology Enablement (OneTrust): Managed the OneTrust onboarding process to reduce burden on staff. Developed an intelligent supplier questionnaire where responses were risk-weighted, dynamically triggering deeper evidence requests as required. Automated supplier engagement with reminders, escalation notices, and non-compliance letters. Built dashboards for real-time visibility of supplier risk.

Integration: Embedded supplier assurance into procurement and contract management lifecycles, with reporting and governance structures established for senior leadership oversight.

The Result

The organisation's supplier assurance process was transformed into a modern, risk-based, ISO 27001-aligned and DTAC-compliant framework. Through OneTrust, assurance became centralised, automated, and scalable. Real-time dashboards gave leaders confidence, intelligent workflows tailored assurance to supplier risk, and automation reduced delays while holding suppliers accountable.

Jason McAdam, Director & Co-Founder of i3Secure commented on the work:

"Cyber attackers increasingly target supply chains, making supplier assurance vital to resilience in healthcare. By combining ISO 27001 and DTAC alignment with OneTrust automation, we created a framework that is both practical and scalable. The client was delighted with the outcome and now has confidence that supplier risks are being managed consistently and transparently."

© 2025 i3Secure Ltd