

CASE STUDY

A large investment fund engaged Crenellate to develop a comprehensive security position paper as part of its investment due diligence for a proposed high-security development.

With an interest in entering the critical infrastructure sector, the fund sought to evaluate the feasibility, risk landscape, and regulatory requirements associated with building a classified computing facility in Australia. Given the stringent security mandates governing such facilities—including compliance with ASIO-T4, the Protective Security Policy Framework (PSPF), and the Information Security Manual (ISM)—the investment group required a structured assessment of security considerations.

Crenellate was engaged to distil complex security requirements into a clear, actionable framework, ensuring the hedge fund had the strategic intelligence necessary to assess investment viability, risk exposure, and long-term operational feasibility.

Should the investment proceed, Crenellate will provide end-to-end security consulting services, ensuring the facility's security framework, governance model, and operational safeguards align with national security requirements and classified computing standards.

CHALLENGE

Investing in a high-security infrastructure presents unique challenges beyond conventional commercial infrastructure. Classified facilities must comply with Australia's strictest security frameworks, requiring physical, cyber, and operational safeguards that significantly impact design, cost, and regulatory obligations.

The fund needed to evaluate the financial and operational feasibility of such an investment but lacked the specialised security expertise required to navigate SSEC standards, sovereign data mandates, and advanced cyber risk mitigation measures. Without a structured security assessment, it was difficult to determine whether the proposed facility would meet the accreditation requirements necessary to host classified workloads.

Beyond compliance, the fund also needed to assess geopolitical risk, market demand, and the competitive landscape for high-security data centre investments. The challenge was to balance security obligations with commercial realities, ensuring the investment was not only technically feasible but also financially viable.

To address these concerns, the fund required a detailed position paper, providing an independent, expert-led security analysis to inform investment decision-making.

SOLUTION

Crenellate developed a comprehensive security position paper, outlining key design considerations, regulatory obligations, and risk factors associated with developing a high-assurance data centre.

The document served as a strategic roadmap, enabling the hedge fund to make an informed investment decision based on practical security implications and compliance feasibility.

The position paper addressed five critical areas of security design and risk mitigation:

- Security Zoning & Access Control – Establishing a multi-tiered security model aligned with SCEC Zone 5 requirements, incorporating biometric authentication, mantrap entry points, and controlled personnel access for highly classified environments.
- Facility Hardening & Threat Mitigation – Evaluating the need for structural reinforcements, intrusion detection systems, and Technical Surveillance Countermeasures (TSCM) to mitigate covert surveillance and unauthorised access risks.
- Cybersecurity & SOC Integration – Assessing Secure Operations Centre (SOC) implementation, real-time network monitoring, post-quantum cryptographic security, and threat mitigation strategies to ensure resilience against state-sponsored cyber threats.
- Regulatory Compliance & Accreditation Pathways – Mapping security controls to ASIO-T4, PSPF, ISM, ASD Essential Eight, and the Australian Government's Hosting Certification Framework, ensuring a clear path to security accreditation.
- Operational Resilience & Business Continuity – Evaluating redundant power, cooling, and environmental threat mitigation, ensuring the facility could withstand geopolitical disruptions, cyberattacks, and infrastructure failures.

By consolidating these security, regulatory, and operational considerations into a single authoritative reference, Crenellate provided the hedge fund with the intelligence needed to assess both the risks and opportunities of the investment.

OUTCOME

Crenellate's position paper enabled the fund to critically assess the viability of investing in a high-security data centre, equipping decision-makers with a clear understanding of security obligations, regulatory complexity, and operational risk factors.

The analysis provided a structured evaluation framework, ensuring the investment team could assess cost implications, compliance feasibility, and potential barriers to market entry. By demystifying security accreditation pathways, the document helped the fund determine whether pursuing the investment aligned with its long-term commercial objectives and risk appetite.

Should the investment proceed, Crenellate will lead the security implementation phase, overseeing the design and deployment of a Secure Operations Centre (SOC), access control systems, and classified computing security measures. The firm will also provide ongoing risk management services, ensuring the data centre maintains continuous compliance with evolving national security standards.

This engagement underscores Crenellate's expertise in high-assurance security strategy, reinforcing its position as a trusted advisor for investors evaluating critical infrastructure opportunities. By bridging investment due diligence with long-term security governance, Crenellate ensures that high-security facilities are not only commercially viable but also operationally resilient in an era of evolving geopolitical threats.

