**Knowledge Series**
maroubraconsulting.com

# Spotlight: IT Security

## When IT security becomes business strategy

**April 2026**
**By Maroubra Consulting**

## IT security certifications as a growth accelerator

IT Security has become a competitive differentiator.

Customers, partners, and investors increasingly expect companies to demonstrate a strong security posture through certifications like ISO 27001 and SOC 2. For many markets and industry segments, these certifications are no longer optional. They have become minimum entry requirements for being considered a credible cooperation partner.

For a given client, proven IT compliance demonstrates operational maturity and reduces perceived risk in procurement processes. For the market-oriented vendor it lowers barriers to entry, shortens sales cycles, opens access to enterprise clients, and strengthens brand trust. Companies that invest in IT certifications consistently experience:

- Higher win rates in competitive bids
- Faster onboarding with enterprise customers
- Greater trust in negotiations and due diligence

In short, security certifies not just systems, but becomes a core component of a business' credibility. Demonstrating compliance to universal security frameworks becomes part of the value proposition, and a direct driver of growth.

### Speed-to-compliance: How can automation and AI help?

Automation and AI combined can be essential to executing an effective compliance strategy in an efficient and effective manner. Implementing security controls manually can slow down progress, introduce errors, and delay certification. AI-enabled monitoring and automated workflows act as a quality assurance engine, ensuring controls are consistently applied and gaps are identified early.

Key use cases:

- Automated evidence collection: removes human error and accelerates audit readiness
- Continuous control monitoring: AI detects misconfigurations or missing vulnerability patches in real time
- Automated user access reviews: ensures correct onboarding/offboarding without delays
- Policy compliance checks: AI validates devices, permissions and configurations in realtime

By shifting from periodic reviews to continuous, automated assurance, companies achieve significantly faster speed-to-compliance, meaning that the commercial benefits of certification can start to count sooner.

From this strategic point of view: Automation and AI don't just support cyber defense, they operationalise the entire compliance strategy.

## IT Security maturity: Where are companies today?

Across our market interviews, several clear maturity patterns emerged:

- Most companies overestimate their security posture, often because they rely heavily on large cloud providers and take IT security for granted. This creates a perception of safety rather than true, evidence-based maturity from the entire operational environment.
- Documentation and routines are weak or missing. Policies exist 'on paper' but are not necessarily implemented across the organisation.
- Risk management, access routines, supplier management, and IT security procedures are often immature.
- Sensitive data exposure is poorly understood. Organisations might think they have 'very little sensitive data', yet these data can easily become sensitive when combined with other sets.
- Physical security and device handling are not up to needed standards

Next becomes: Why are many firms lagging on IT security? Capacity seems to be a major challenge: Most teams have not invested sufficiently in organisational capacity to handle IT security or compliance strategy. Even companies with strong technical teams struggle with employee awareness, documentation, and process-heavy aspects of IT security.

Finally, the adoption of ISO27001 and SOC2 certifications lag behind market expectations. Awareness has increased, but adoption rates of these compliance frameworks are still relatively low. The gap between client expectations and actual security maturity actually seems to be widening.

## The risk of leaving IT security out of the strategic roadmap

When IT security is not anchored in the long-term strategic roadmap, organisations face a widening gap between market expectations and their actual investment in IT security readiness.

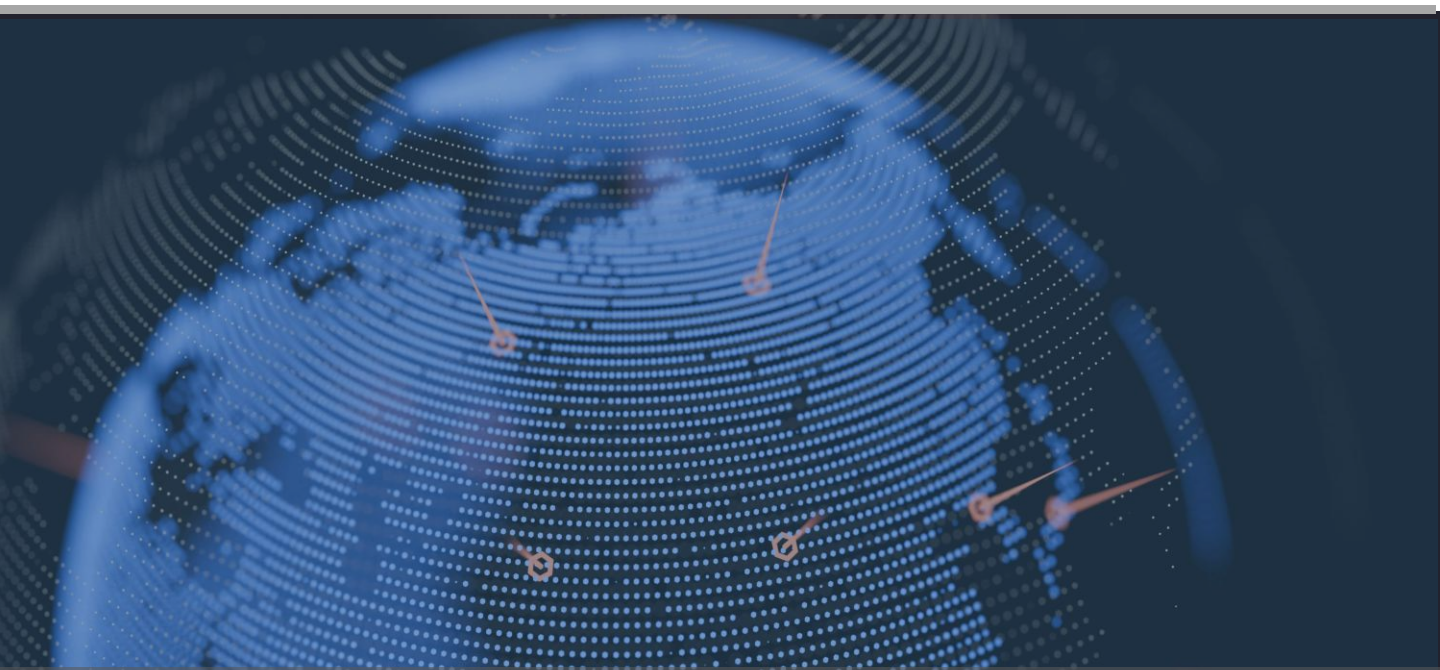
Customers, partners, and investors increasingly use security maturity and certifications as a proxy for credibility; without ISO27001 or SOC2, companies lose deals, struggle in procurement processes, and appear less reliable during due-diligence conversations.

Internally, weak routines, missing documentation, and inconsistent data handling create a reactive security posture, leaving the organisation exposed to misconfigurations, vendor mistakes, and preventable incidents.

Companies that postpone security also delay their certification timeline, pushing back the commercial benefits that come with it, from enterprise access to shorter sales cycles and smoother onboarding.

Over time, this creates a compounding disadvantage: Competitors who invest early gain a trust advantage, integrate automation and AI into their controls, and achieve faster speed-to-compliance, allowing them to unlock market opportunities far sooner.

**Knowledge Series**
maroubraconsulting.com



**About Maroubra Consulting**

Maroubra Consulting is an international management consulting firm, specialists in operational excellence. The company supports client organisations with improving competitiveness, strengthening operational resilience and achieving sustainable growth. With a ‘global-first’ and ‘remote-first’ business model, and market presence in Bergen, Barcelona, Amsterdam, San Francisco and Sydney, Maroubra Consulting combines strategic direction with digital innovation. The company proudly support the United Nations Sustainable Development Goal #1: No Poverty, partnering with NGOs to create lasting impact.