# IMPACTO Model Frequently Asked Questions

**1. Does IMPACTO help an organization decide which cybersecurity product to purchase?**

No. The IMPACTO Model assumes a cybersecurity solution has already been selected and acquired. Its primary focus is *post-purchase optimization* to ensure the investment delivers measurable value, aligns with the organization’s risk tolerance, and evolves with changing threats.

**2. Is IMPACTO replacing frameworks such as NIST CSF, C2M2, or SOC-CMM?**

Not at all. IMPACTO is intended to *complement* established frameworks by providing a **stage-based lifecycle** for maximizing the value of existing cybersecurity solutions after purchase. Many organizations use NIST CSF, C2M2, or SOC-CMM for broader program or SOC maturity tracking; IMPACTO can integrate seamlessly to accelerate the maturity and capability outcomes prescribed by those frameworks.

**3. How does IMPACTO address smaller organizations with limited staffing or budgets?**

The IMPACTO Model is *scalable*. Smaller teams can adopt the same six stages (0–5) with lighter-weight processes and fewer specialized roles. For example, documentation might be simplified runbooks, and training may involve short, targeted sessions rather than formal certification tracks. The goal remains to ensure each purchase delivers meaningful risk reduction within the constraints of a given environment.

**4. Can IMPACTO be used for hardware- and cloud-based solutions, or is it restricted to software?**

IMPACTO is designed to be flexible and *technology-agnostic*. It applies to various cybersecurity investments, such as hardware appliances (firewalls or network sensors), software tools (SIEM or EDR), managed services, or cloud-based controls. Each stage’s core principles (e.g., clarifying business alignment, defining roles, standardizing processes, integrating advanced analytics) remain the same across technology types.

**5. Does the model require advanced risk quantification like FAIR or NIST SP 800-30?**

IMPACTO encourages *risk-informed decisions* but does not mandate a specific methodology. Organizations can use FAIR, NIST SP 800-30, or simpler “rapid risk audits.” The important requirement is that risk reduction (ARP vs. PRP) be tracked consistently throughout the stages, regardless of which quantitative or qualitative approach is preferred.

**6. Can only parts of IMPACTO be adopted, or must all six stages be followed strictly?**

The model is designed as a *holistic lifecycle*, but partial adoption is feasible. Some organizations may already meet many Stage 2 or 3 criteria and only need selected elements from those stages. However, fully following the progression from Stage 0 (Purchased) through Stage 5 (Optimizing) often reveals overlooked gaps and opportunities that partial adoption might miss.

**7. How is the return on investment (ROI) measured with IMPACTO?**

Each stage emphasizes *tangible metrics*, including cost avoidance (reduced incident impacts), mean-time-to-detect (MTTD), and mean-time-to-respond (MTTR) improvements or more sophisticated calculations such as annual loss expectancy (ALE). These metrics provide a basis for demonstrating ROI to leadership and justifying further investments or expansions.

**8. Does the organization need a minimum maturity level to use IMPACTO?**

IMPACTO begins at **Stage 0 (Purchased)**, which requires only that a purchase has been made. Even if the overall security maturity is low and the solution is still “shelfware,” the model’s step-by-step approach helps move from minimal usage to fully optimized integration.

**9. What if the organization already implements multiple security solutions?**

Organizations with multiple products or services can apply IMPACTO *individually* to each critical purchase or bundle them into a collective roadmap. The framework’s principles in either approach—defining purchased vs. actual capabilities, tracking risk, and iterating through maturity stages—remain consistent.

**10. Is there any guidance regarding future expansions or updates to IMPACTO?**

Since this is the *first version* of the IMPACTO Model, additional guidance is anticipated as more organizations adopt and provide feedback. Future iterations may include domain-specific best practices, more profound case studies, and expanded examples of how to map IMPACTO to emerging regulatory requirements or security innovations.

**11. Does IMPACTO incorporate guidance from the NZ NCSC Investment Approach for determining the Business domain stage?**

Yes. The IMPACTO Model aligns well with the NZ NCSC’s cyclical approach (Know the Landscape, Define the Strategy, Deliver Results, Measure Success). Organizations can apply NCSC principles (e.g., business alignment, ROI justification, metrics) to assess how effectively an investment supports broader strategic objectives—directly informing the Business domain rating in IMPACTO.