# IMPACTO Model At-a-Glance

**1. Purpose and Scope**

The Integrated Maturity, Program Acceleration for Cyber Transformation & Optimization (IMPACTO) Model is a structured, post-purchase cybersecurity framework designed to transform your cybersecurity investments into strategic business enablers. Its objective is to optimize solutions you have already acquired, ensuring measurable risk reduction, clear alignment with business goals, and demonstrable ROI.

**Primary Goal:** Move beyond basic tool implementation ("shelfware") to a fully optimized, strategic cybersecurity capability that continuously adapts to evolving threats and organizational objectives.

**Key Principle:** Cybersecurity investments should deliver clear business outcomes, quantified through reduced risk and operational impact, going beyond mere compliance.

**2. High-Level Approach**

IMPACTO comprises six maturity stages (0–5) across four domains:

* **Business** – Budget alignment, executive sponsorship, strategic goal mapping, risk quantification (ROI, ALE)
* **People** – Clearly defined roles, competency frameworks (e.g., NIST NICE), ongoing training
* **Process** – Formalized workflows, SOPs, incident response runbooks, governance, continuous improvement
* **Technology** – Tool configurations, advanced integrations, analytics, MITRE ATT&CK/D3FEND alignment

**Stages 0–5:**

* **0: Purchased** – Minimal deployment, unclear business rationale, “shelfware”
* **1: Ad Hoc** – Sporadic use, basic compliance-driven activities, minimal documentation
* **2: Managed** – Defined tasks, documented runbooks, clear roles established
* **3: Formalized** – Integrated security into broader organizational workflows, systematic improvements
* **4: Data-Driven** – Advanced metrics and analytics drive proactive security decisions, reduced false positives
* **5: Optimizing** – Real-time adaptation, continuous intelligence-driven improvements, strategic business enabler

**How It Works:**

* Evaluate each domain’s current maturity stage
* Identify domain-specific gaps (e.g., incomplete training, insufficient runbooks, inadequate ROI metrics)
* Implement recommended practices to progress systematically through higher stages

**3. How to Use the IMPACTO Model**

* **Assess Current State:** Identify your stage (0–1 for new or minimally deployed tools, stage 2–3 for partially integrated solutions)
* **Domain Mapping:** Evaluate Business, People, Process, and Technology maturity independently
* **Apply Classification Frameworks:**
  + **Maturity Classification Framework (MCF):** Evaluates consistency and improvement of people and processes
  + **Capability Classification Framework (CCF):** Measures depth of tool deployment and utilization
* **Leverage Operational Intelligence (OI):** Use real-world threat intelligence, incident data, and scenario testing to adjust capabilities continuously
* **Continuous Improvement:** Regularly reassess domains, measure progress with KPIs (MTTD, MTTR), and iterate to higher maturity stages

**4. Key Disclaimers**

* **Post-Purchase Focus:** IMPACTO is not for selecting cybersecurity products; it maximizes the value of existing investments.
* **Complementary Framework:** Complements existing standards (NIST CSF, SOC-CMM, Zero Trust), facilitating practical operationalization.
* **Scalability:** Applicable across organizational sizes—from small teams to global enterprises—with scalable documentation and processes.
* **Evolving Model:** Version 0.1 is an evolving model. Future updates will refine domain criteria, practices, and integration with emerging standards and regulatory frameworks.
* **Risk Methodology Agnostic:** Compatible with various risk methodologies (FAIR, NIST SP 800-30). The model emphasizes consistent tracking of purchased versus actual risk outcomes.