The IMPACTO Model

Integrated Maturity, Program Acceleration for Cyber Transformation and Optimization

*A Roadmap to Optimize Cybersecurity Investments*

*and Realize Strategic Value*

By Kyle Villano

Version 0.1

© 2025 Kyle Villano – This document is part of the IMPACTO Model project and is licensed under the Creative Commons Attribution‑ShareAlike 4.0 International License (CC BY‑SA 4.0). To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/>

Table of Contents

[Preface 3](#_Toc194163292)

[Purpose and Scope 4](#_Toc194163293)

[Foundational Principles 6](#_Toc194163294)

[Core Stages of the IMPACTO model 7](#_Toc194163295)

[Domains 7](#_Toc194163296)

[Stages 9](#_Toc194163297)

[Determining the Overall Stage Value 20](#_Toc194163298)

[Classification Frameworks 21](#_Toc194163299)

[Maturity Classification Framework (MCF) 21](#_Toc194163300)

[Capability Classification Framework (CCF) 21](#_Toc194163301)

[Integrating MCF and CCF 22](#_Toc194163302)

[Unified Assessments 22](#_Toc194163303)

[Capability Profiles 23](#_Toc194163304)

[Purchased Capability Profile (PCP) 23](#_Toc194163305)

[Actual Capability Profile (ACP) 24](#_Toc194163306)

[Operating Context 25](#_Toc194163307)

[Purchased Operating Context (POC) 25](#_Toc194163308)

[Actual Operating Context (AOC) 26](#_Toc194163309)

[Risk Profiles 27](#_Toc194163310)

[Purchased Risk Profile (PRP) 27](#_Toc194163311)

[Actual Risk Profile (ARP) 27](#_Toc194163312)

[Risk Quantification Tool/Methodology (RQT) 28](#_Toc194163313)

[Operational Intelligence 30](#_Toc194163314)

[Initial Momentum and Progressing Stages 32](#_Toc194163315)

[Operationalizing the Purchase Stage 32](#_Toc194163316)

[Vendor and Professional Services Collaboration 35](#_Toc194163317)

[Visualization and Reporting 36](#_Toc194163318)

[Service Roadmap and AI-Assisted Planning 36](#_Toc194163319)

[Key Terms and Acronyms 37](#_Toc194163320)

[References 40](#_Toc194163321)

# Preface

Organizations often assume that a newly purchased cybersecurity solution will deliver the exact risk reduction and capabilities promised during procurement. In practice, these *purchased* assumptions frequently diverge from *actual* outcomes. Once real-world incidents, staffing changes, and environmental factors come into play, the purchased assumptions may diverge, often prompting repeated adjustments.

The IMPACTO Model is designed to transform cybersecurity investments into dynamic, strategic assets that drive lasting change. IMPACTO is a structured approach that drives **Program Optimization** from initial purchase to a fully **optimized** security program (*Stage 5*). Peter Drucker wisely noted, “*The best way to predict the future is to create it.*” This insight encapsulates the proactive spirit at the heart of the IMPACTO Model. Rather than accepting security as a static cost center, the model challenges leaders to design and build a future-proof security posture that evolves with the evolving threat landscape.

By following the IMPACTO Model’s roadmap, organizations align their investments with clear, quantifiable business goals and risk metrics from the very beginning. Every dollar spent is directed toward reducing threat exposure and enhancing operational resilience. As the model guides the journey from an initial cybersecurity purchase to a fully optimized capability, it fosters a continuous assessment, refinement, and improvement cycle.

**IMPACTO does not offer guidance on which product to purchase. It is a post-purchase model designed to maximize and measure the value of an already selected cybersecurity investment.**

The model is primarily focused on the following audience and roles:

|  |  |
| --- | --- |
| **Role** | **Rationale** |
| **Security Leaders & CISOs** | Demonstrate the return on existing cybersecurity investments and secure the ongoing budget. |
| **Product Owners & Tool Champions** | Drive structured deployment and continuous improvement, ensuring purchased features are utilized effectively. |
| **Professional Services & VARs** | Align engagements to each IMPACTO Model stage to accelerate client outcomes. |
| **Financial Officers & Executive Boards** | Get tangible, risk-based insights (ALE, ROI) that support budget and resource allocation for post-purchase optimization. |

# Purpose and Scope

Organizations today cannot afford to view cybersecurity as a siloed cost center; instead, it must be a strategic, value-driven pillar of their overall mission. The **Integrated Maturity, Program Acceleration for Cyber Transformation & Optimization (IMPACTO) Model** provides a structured, multi-stage framework that ensures every security purchase is grounded in measurable outcomes and aligned to core business goals.

A key driver behind IMPACTO is the imperative to realize value quickly. By mapping purchased solutions to tangible risk-reduction metrics (e.g., annualized loss expectancy) and clearly defined capabilities (e.g., coverage of key MITRE ATT&CK techniques), organizations can accelerate deployment timelines, shorten learning curves, and see early returns. This reduced time-to-value enhances operational resilience and demonstrates quantifiable progress to boards and senior leadership, building confidence in the security program’s ongoing investments.

**Why It Matters**

* **Clear, Quantifiable Risk vs. Return -** Leadership can leverage the IMPACTO Model’s emphasis on data-driven risk assessments, aligning each cybersecurity investment with documented risk reductions and business outcomes.
* **Actionable Investment Pathways -** A multi-stage roadmap helps executives prioritize deployments, professional services engagements, and training schedules in a logical, high-impact sequence.
* **Evidence-Based Accountability—**Standardized rubrics, combining a Maturity Classification Framework (MCF) and a Capability Classification Framework (CCF), ensure consistent and transparent reporting. This fosters trust with stakeholders and external assessors.
* **Adaptability to Strategic Shifts -** As business priorities evolve or new threats emerge, IMPACTO’s iterative updates to the Actual Risk Profile (ARP) enable quick people, processes, and technology recalibration.

**How This Document Helps**

* **Guidance from Purchase to Optimization -** It offers concrete steps for evolving from the initial tool purchase (Stage 0) to a fully optimized security program (Stage 5).
* **Alignment With Recognized Frameworks -** Common standards (e.g., NIST CSF, MITRE ATT&CK) are referenced to ensure broad applicability and easier stakeholder buy-in.
* **Business Value Realization -** By embedding risk quantification, capability tracking, and continuous improvements, IMPACTO aligns cybersecurity investments with real, measurable business benefits—elevating security from a compliance necessity to a strategic enabler.

**Integrating a Structured Investment Approach**  
Drawing on guidance from the New Zealand National Cyber Security Centre (NZ NCSC), cybersecurity investments can be viewed as a cyclical and iterative process rather than one-time expenditures. This approach emphasizes four key phases—identifying the risk landscape, defining a clear strategy, delivering tangible results, and measuring success—to ensure each investment aligns with organizational goals and achieves measurable risk reduction. By harmonizing these phases from the NZ NCSC with the IMPACTO Model’s multi-stage roadmap, organizations can more confidently determine how each security purchase contributes to their overall mission and reevaluate priorities when threats change, or budget constraints shift.

For instance, the NCSC framework underscores the need to “start with the business in mind,” which aligns with IMPACTO’s principle of mapping every purchase (Stage 0) to the broader corporate objectives and risk profile. At the same time, continuous re-assessment (akin to IMPACTO’s Stage 5) helps decision-makers confirm that acquired capabilities remain aligned with strategic outcomes and deliver ongoing value. If weaknesses persist, leadership has clear visibility to correct course without undermining other security investments (National Cyber Security Centre [NCSC], 2023).A diagram of a business transformation

AI-generated content may be incorrect.

# Foundational Principles

The IMPACTO Model is built on five Foundational Principles, underpinning the journey from a mere cybersecurity purchase to a fully optimized security program. The following diagram highlights how these principles reinforce one another to drive measurable risk reduction and long-term business value.

A diagram of a company's impact

AI-generated content may be incorrect.

By embedding these Foundational Principles into every stage of the IMPACTO Model—from initial purchase to complete optimization—organizations ensure that each cybersecurity investment is systematically aligned with business goals, operational workflows, and measurable risk outcomes. The following sections illustrate how these principles apply within each IMPACTO Domain and Stage.

# Core Stages of the IMPACTO model

The IMPACTO Model outlines a six-stage journey, starting from an unstructured purchase (Stage 0) and culminating in a fully optimized security environment (Stage 5) related to the target cybersecurity investment(s). These stages ensure that Purchased Capability Profiles (PCP) evolve into Actual Capability Profiles (ACP) in line with changing risk conditions, newly acquired Operational Intelligence (OI), and shifts in the deployed operating context (POC to AOC). Throughout these stages, organizations utilize the Maturity Classification Framework (MCF) and the Capability Classification Framework (CCF) to measure progress, with the Purchased Risk Profile (PRP) and Actual Risk Profile (ARP) illustrating how investments reduce risk over time.

**This section includes:**

* **High-Level Summary:** A brief overview of each stage and its impact on residual risk.
* **Illustrative Use Cases:** Real-world examples that demonstrate common scenarios.
* **Detailed Stage Descriptions:** Domain-specific criteria, indicators, and business value outcomes.

Reading through this section helps an organization assess its current stage and prepare to transition to higher maturity levels.

## Domains

The table below illustrates the four domains and their focus:

|  |  |
| --- | --- |
| **Domain** | **Focus** |
| **Business**  **(Primarily**  **MCF-Driven)** | * Focuses on budgets, risk quantification (e.g., ALE), executive sponsorship, and alignment with strategic objectives * Ensures that every cybersecurity purchase maps to measurable outcomes and organizational goals |
| **People**  **(Primarily**  **MCF-Driven)** | * Encompasses roles, responsibilities, and necessary skills or training * Example frameworks: NIST NICE for security roles; internal HR frameworks for competency tracking |
| **Process**  **(Primarily**  **MCF-Driven)** | * Encompasses incident response runbooks, workflow definitions, standard operating procedures (SOPs), and governance structures * Tracks how consistently procedures are documented, tested, and improved |
| **Technology**  **(Primarily**  **CCF-Driven)** | * Covers the actual tools, configurations, integrations, and advanced features used to detect and respond to cyber threats * Relies heavily on recognized frameworks (e.g., MITRE ATT&CK, D3FEND) to gauge coverage and technical depth |

These four domains move in tandem through the IMPACTO Stages (0–5), shaping an organization’s overall security maturity and capability.

NCSC’s *Cyber Security Investment: A Structured Approach* outlines a clear cycle—Know the Landscape, Define the Strategy, Deliver Results, and Measure Success—to align cyber spending with organizational objectives. Within IMPACTO, this framework informs how mature an investment’s **Business** domain is:

1. **Know the Landscape**  
   Identify priority risks to core assets. If the purchase was ad hoc and not tied to top business risks, the Business domain typically remains at **Stages 0–1**.
2. **Define the Strategy**  
   Secure executive sponsorship and budget alignment. Multi-year financial planning, cost-benefit analyses, and clear strategic goals often position the Business domain at **Stage 3** or beyond.
3. **Deliver Results**  
   Demonstrate ROI and risk reduction through well-scoped business cases. When usage metrics and incident reporting are routine, the Business domain generally falls into **Stages 2–3.**
4. **Measure Success**  
   Leverage metrics and dashboards to connect cyber investments with broader business outcomes, such as brand reputation and new market opportunities. Consistent, data-driven performance tracking typically indicates **Stages 4–5**.

Using the NCSC’s principles to evaluate these indicators helps pinpoint the maturity of the Business domain. In turn, this rating—whether determined by IMPACTO’s lowest-domain, weighted-average, tiered-threshold, or recommended two-step approach—reveals how effectively leadership justifies and budgets each investment, aligns it with strategic outcomes, and measures its actual business value in practice.

The following tables show how each of the other domains is generally evaluated in the model:

|  |  |
| --- | --- |
| **People** | * Examines whether roles and responsibilities are clearly defined, staff possess the necessary skills, and training paths are in place. * Higher domain stages (Stage 3 or above) typically require structured onboarding, formal succession, and skills development plans—key elements measured by a well-defined MCF. |
| **Process** | * Focuses on procedural consistency, runbook documentation, incident response workflows, and continuous improvement cycles. * Moving from ad hoc (Stage 1) to managed or formalized processes (Stage 2 or 3) indicates that the MCF’s criteria (e.g., documented SOPs, scheduled audits, post-incident reviews) are being met. |
| **Technology** | * Evaluates coverage and completeness of the investment’s capabilities—whether the features have been fully deployed, integrated, and optimized. * A high stage typically indicates advanced usage of the tool’s detection and mitigation features, alignment with frameworks such as MITRE ATT&CK or D3FEND, and ongoing tuning based on operational intelligence (OI). |

## Stages

Below is a concise overview of the progression that sets the stage for the High-Level Summary table. Each successive phase builds on the prior one, advancing from a minimal deployment with limited value to a robust, continuously improving program that delivers measurable risk reduction and strategic return:

Stage 0 begins immediately after purchase, often leaving the solution idle (“shelfware”) with no formal business case or assigned operators. Stage 1 moves to sporadic use—fulfilling basic compliance needs but still lacking structured responsibilities and documentation. At Stage 2, more defined budget planning and role clarity emerge, supported by documented runbooks that facilitate consistent day-to-day operations. Stage 3 focuses on formalized integration, incorporating security objectives into mission-critical goals, training staff to handle advanced threats, and implementing feedback loops to enhance performance after each incident. By Stage 4, data-driven practices take center stage, ensuring that risk modeling informs both strategic decisions and the optimization of technical capabilities. Finally, Stage 5 epitomizes a fully optimized solution: security meets or undercuts initial risk targets and functions as a long-term competitive asset that adapts in near real-time to the evolving threat landscape.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Stage** | **Business** | **People** | **Process** | **Technology** | **Risk Impact** |
| **0 - Purchased** | No formal return-on-investment (ROI) or budget alignment is provided beyond the initial purchase. | No assigned roles or clear responsibilities have been established for the newly acquired cybersecurity investment. | No procedures or documentation; the solution sits idle as potential “shelfware.” | Deployed minimally (or not at all) using default or incomplete configurations. | Negligible security benefit; the purchased risk reductions remain theoretical and unrealized. |
| **1 – Ad Hoc Deployment** | Rudimentary justification (e.g., “We had to meet some security requirement”) | One or two individuals have partial accountability, but staff have no clear training pathways. | Highly reactive approaches, with occasional event or incident checks; no standardized workflows. | Basic setup or integration with limited features, primarily addressing only apparent or commodity threats. | Slight improvement in visibility; actual residual risk barely differs from the initial purchased risk profile. |
| **2 – Managed Deployment** | Budget includes some operational costs; risk quantification is starting to shape justifications. | Well-defined tasks and job descriptions; initial alignment with at least one recognized skill or role framework. | Standard operating procedures exist for recurring tasks; staff follow consistent runbooks for typical scenarios. | Core features are configured; moderate automation or alerting is in place. | Moderate risk reduction as incident handling becomes more consistent; business case for continued investment is more evident. |
| **3 – Formalized Integration** | Security objectives are directly tied to broader organizational goals; risk analysis informs resource decisions. | Roles and competency expectations are clearly defined; advanced or specialized training is implemented where relevant. | Incident reviews and root-cause analyses lead to continuous updates in processes; formal feedback loops exist. | Solutions or services are integrated with analytics or correlation functions to detect a range of threats; automation is regularly employed. | High risk reduction; data-driven metrics validate progress, and residual risk drops in a measurable, repeatable fashion. |
| **4 – Data-Driven Solution** | Detailed risk modeling (e.g., FAIR or internal frameworks) guides decision-making; security is factored into strategic plans. | Roles may include specialized analysts or third-party experts focused on advanced threat detection, hunting, or forensics. | KPI/KRI thresholds and dashboards steer proactive improvements (e.g., patch cadence, threat updates, compliance triggers). | Broad technical interoperability; real-time analytics and correlation reduce both false positives and missed detections; robust automation. | Significant drop in residual risk; real-time metrics allow regular benchmarking of actual vs. purchased risk. |
| **5 – Optimizing Solution** | Security is recognized as a strategic advantage or market differentiator; leadership actively promotes program success. | Teams (internal or external) rotate responsibilities to maintain and grow expertise; industry engagement is common. | Processes adapt in near–real-time based on global threat intelligence and continuous testing; continuous improvement is cultural. | Fully orchestrated environment or integrated services; ongoing improvements and dynamic updates ensure minimal dwell times or blind spots. | Transformative impact; residual risk remains consistently at or below target levels, showcasing definitive ROI over the long term. |

**Stage 0 – Purchased**

The cybersecurity solution has already been acquired, yet no significant setup or operational procedures have been established. Stage 0 addresses the initial ownership assignment, minimal configuration tasks, and preliminary clarification of the risk or capability outcomes that motivated the procurement. This phase ensures the newly purchased product does not remain on the shelf indefinitely but serves as the foundation for subsequent, value-driven stages.

| **Domain** | **Criteria** | **Indicators** |
| --- | --- | --- |
| **Business** | - No comprehensive business case or financial planning beyond the initial purchase.  - Vague or non-existent risk metrics (purchased risk reduction is unclear). | - Executives or responsible managers unsure why the tool/service was bought (“Someone said we needed it…”).  - No formal tracking or reporting of potential value or alignment to company goals. |
| **People** | - No designated individuals or service providers are truly responsible for setup or operation.  - No training plan or even awareness of the solution’s full scope. | - One overwhelmed person or an external vendor contact may be tangentially aware of the product but lacks authority or expertise to implement.  - No references to skill or competency frameworks. |
| **Process** | - Zero to minimal documentation on how this solution will be integrated (no standard operating procedures).  - Ad hoc reaction if issues or alerts arise. | - Informal or no runbooks; if something goes wrong, it’s handled via scattered emails or calls.  - No thought given to how the solution might impact incident response or threat monitoring. |
| **Technology** | - The product or service is partially deployed or not deployed at all; default configurations are left untouched.  - No integration with the broader environment. | - It could be “shelfware” or simply turned on with default settings, offering no meaningful protection.  - No advanced features enabled; limited or no telemetry flowing in or out. |
| **Business Value** | **Negligible.** Money has been spent without translating into genuine security gains. |  |

**Stage 1 – Ad Hoc Deployment**

Stage 1 marks the first efforts to utilize the newly purchased solution ad hoc. Essential activation and intermittent monitoring may occur at this juncture, usually with minimal documentation and loosely assigned roles. The activities remain highly reactive, making Stage 1 a necessary starting point for more structured and consistent practices in the later stages.

| **Domain** | **Criteria** | **Indicators** |
| --- | --- | --- |
| **Business** | - Basic rationale for use (e.g., to address a single regulation or compliance item).  - Budget may cover immediate support costs but with no clear multi-year outlook. | - Short statements in leadership slides (“It’s for compliance”).  - Renewals are uncertain or not discussed beyond immediate needs.  - Risk acknowledgments are mostly informal (“We need to reduce attacks”). |
| **People** | - One or two individuals (or a single external vendor) handle everything on a part-time basis.  - No defined skill framework or competency plan for operating the tool. | - No official training beyond basic product demos.  - Staff or providers express confusion about roles/responsibilities; no escalation plan for complex incidents.  - Slow or unclear triage of security events. |
| **Process** | - Highly reactive processes; incident handling relies on ad hoc steps.  - Minimal or isolated data collection; inconsistent logs or partial visibility. | - Some detection events may be noticed, but there is no formal incident-handling procedure.  - “Lessons learned” rarely captured, improvements happen after problems but remain undocumented or inconsistent. |
| **Technology** | - Tool/Service is technically “on” but configured with minimal tuning or correlation.  - It addresses only the most basic or obvious malicious activities. | - Out-of-the-box settings remain; advanced configurations are untouched.  - Occasional quick wins (e.g., blocking a known bad IP), but overall coverage and integration are superficial. |
| **Business Value** | **Low**  Some incremental compliance or visibility gains are there, but the gap between purchased risk goals (PRP) and actual risk reduction (ARP) remains large. |  |

**Stage 2 – Managed Deployment**

Building on the ad hoc operations of Stage 1, Stage 2 introduces more defined tasks, assigned responsibilities, and documented processes. The organization begins to deploy the solution regularly for threat detection and response. By establishing these managed practices, the deployment framework becomes reliable enough to underpin the deeper integration and optimization that will follow in advanced stages.

| **Domain** | **Criteria** | **Indicators** |
| --- | --- | --- |
| **Business** | - Clearer link between investment and risk scenarios (e.g., phishing, ransomware).  - Multi-year budgets or renewal planning start to include operating costs. | - Leadership requests or receives basic usage/incident reports.  - Possible inclusion of simple risk quantification (e.g., “We lowered email breach risk by X%”).  - More formal proposals for additional funding or expansions. |
| **People** | - Formal roles defined for operations (in-house or with an external security provider).  - Some alignment to recognized skill/role frameworks; minimal training is funded. | - Staff or service providers use documented roles (“Tier 1 analyst,” “Incident coordinator,” etc.).  - Training or upskilling budgets become part of the conversation.  - Fewer single points of failure. |
| **Process** | - Standard runbooks or procedures exist for recurring events (e.g., common incident types).  - Basic post-incident reviews occur, but are still somewhat reactive. | - Documented steps for triaging typical alerts (e.g., suspicious login attempts).  - Occasional “lessons learned” sessions that refine runbooks, though not exhaustive or deeply systematic. |
| **Technology** | - Key features are enabled and integrated (to some extent), providing consistent detection/alerting.  - Automation or correlation is limited but exists for known threats. | - Analysts or providers can keep up with daily alerts without manual overload.<br/>- Basic thresholds or event correlation for frequently observed attacks.  - Reduced missed events for commodity threats. |
| **Business Value** | **Moderate**  Moderate. Incident handling is more organized and risk reduction becomes apparent enough to justify ongoing resource allocation. |  |

**Stage 3 – Formalized Integration**

Stage 3 moves beyond managed processes to a more rigorous, formalized integration. The organization systematically embeds the solution into established workflows, runbooks, and training programs, leveraging the baseline usage data and more precise product insights obtained in previous stages. At this level, addressing discrepancies between the purchased capability profile (PCP) and the actual capability profile (ACP) becomes a core objective, ensuring the solution is aligned with defined risk objectives and performance expectations.

| **Domain** | **Criteria** | **Indicators** |
| --- | --- | --- |
| **Business** | - Security goals explicitly map to the organization’s mission and objectives.  - Regular use of risk metrics (could be ALE or other frameworks) to influence budgets and decisions. | - Risk data is discussed at leadership or board meetings; spending decisions reference measurable outcomes.  - ROI or business impact analyses tie security to operational or strategic benefits.  - Ongoing expansions or renewals guided by risk-based reviews. |
| **People** | - Detailed competency requirements exist (aligned to NIST NICE, internal frameworks, or external service-level commitments).  - Specialized training (e.g., advanced threat analysis) is offered or required. | - Staff or service providers exhibit defined career paths; turnover decreases due to professional growth.  - Certifications or targeted skill-building programs reduce reliance on a small cadre of experts. |
| **Process** | - Comprehensive runbooks are maintained for a range of scenarios; formal post-incident analyses drive continuous updates.  - Rapid adaptation to new threats or advisories. | - Larger or more complex incidents see thorough root-cause analysis (RCA) that leads to documented process improvements.  - Feedback loops exist—what’s learned in each incident shapes the next iteration of runbooks or workflows. |
| **Technology** | - Integrated solutions or service layers handle more advanced threats; increased automation for repetitive tasks.  - Broader coverage of assets (cloud, on-prem, remote, etc.). | - Multi-layered detection or correlation with fairly robust tuning; false positives begin to drop.  - External threat data (or external specialized services) is integrated to catch emerging attack patterns. |
| **Business Value** | **High**  Risks are noticeably reduced, validated by measurable data. The business views security as a valuable operational pillar rather than mere overhead. |  |

**Stage 4 – Data-Driven Solution**

With the solution firmly established, Stage 4 emphasizes extensive metrics, analytics, and operational intelligence to guide iterative improvements. Advanced risk quantification (ARP) and deeper technical configurations (ACP) inform strategic decisions and operational adjustments. Rather than relying on routine tool usage, the organization now embraces continuous improvement supported by near real-time data and robust analytical insights.

At Stage 4, organizations leverage advanced threat intelligence frameworks like \*\*MITRE D3FEND\*\* to pinpoint specific defensive strategies aligned with adversary TTPs (Tactics, Techniques, and Procedures). This level of intelligence-driven coverage allows teams to:

- Cross-reference real-time intel feeds against known TTPs.

- Adapt detection logic quickly to emerging attack patterns.

- Perform targeted hunts for threats that align with newly discovered TTPs.

These proactive measures reinforce the “Data-Driven” concept, ensuring security teams base their priorities on threat intelligence data rather than purely reactive alerts.

| **Domain** | **Criteria** | **Indicators** |
| --- | --- | --- |
| **Business** | - Advanced risk quantification models drive cybersecurity strategy and budget (e.g., scenario-based, ALE-like, or proprietary frameworks).  - Security is woven into broader organizational or product roadmaps. | - Leadership dashboards track real-time KRIs/KPIs; business units factor security data into major initiatives.  - Data-driven cost-benefit analyses for new security initiatives or expansions.  - Security increasingly seen as part of the brand’s reliability or trust value. |
| **People** | - Specialized roles may include data analytics, threat hunting, or advanced forensics, whether in-house or through a managed partner.  - Team performance and skill gaps are regularly measured. | - Staff (or providers) monitor advanced metrics, such as mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).  - Immediate adjustments in staffing or outsourced services occur when metric thresholds are not met.  - High morale from clear performance indicators. |
| **Process** | - KPI/KRI frameworks are used to proactively refine processes (e.g., triggering patch cycles if certain threat levels spike).  - Detailed compliance or regulatory mapping is easily reported. | - Regular internal audits or compliance checks show few to no major gaps.  - Trend analysis of detection accuracy, dwell time, and alert volumes prompts quick iteration of runbooks.  - The organization can pivot quickly on new threats or vulnerabilities. |
| **Technology** | - Extensive interoperability among cybersecurity tools/services with near real-time correlation; advanced analytics or machine learning may be leveraged  - Frequent testing (e.g., breach simulations) ensures coverage. | - Alerts are high-fidelity; false positives are significantly reduced.  - Tools or providers are pushing advanced features or integrations (e.g., cross-platform correlation, advanced behavioral analysis).  - Timely updates or expansions reflect new threat intelligence. |
| **Business Value** | **Significant**  The organization measures a clear drop in residual risk; consistent data and reporting reinforce the decision-making process and underwrite new strategic initiatives. |  |

**Stage 5 – Optimizing Solution**

Stage 5 represents the pinnacle of post-purchase maturity, where the solution is fully integrated across all relevant processes and continuously refined through real-time analytics. This phase elevates the purchased tool to a strategic enabler, actively adapting to emerging threats and aligning with evolving business imperatives. The emphasis on ongoing updates, measurable risk reduction, and sustained ROI M3TID focuses on threat intelligence analysis and real-time detection updates. MITRE D3FEND provides a catalog of defensive techniques. Integrating both allows organizations to adapt quickly (M3TID) and systematically enhance coverage of adversary TTPs (D3FEND). Typical practices at this level include:

- Enrich security analytics with a deep context of adversary motivations and techniques.

- Automating the application of newly discovered indicators of compromise (IOCs) or TTP signatures.

- Continuously refining playbooks in response to fresh threat intel, ensuring minimal dwell time.

At this mature stage, threat intelligence is an ongoing feedback loop—informing continuous improvements in processes (runbooks) and technology (detection rules) to keep pace with advanced adversaries.

| **Domain** | **Criteria** | **Indicators** |
| --- | --- | --- |
| **Business** | - Security is actively marketed or recognized as a competitive differentiator; it supports new ventures or partnerships.  - Renewals and expansions are proactively synced with emerging needs and threats. | - Executive-level references to security in investor or shareholder discussions, or as part of brand identity.  - Cyber risk metrics factor into major corporate milestones (new product lines, mergers, expansions).  - Management invests with confidence in next-gen improvements. |
| **People** | - Continual learning and rotation of responsibilities ensure fresh perspectives; staff or providers are recognized as industry experts.  - Collaboration extends beyond security teams to the entire organization. | - Ongoing skill development, cross-functional collaboration with DevOps, product teams, or external suppliers.  - Attracting and retaining high-caliber talent or top-tier vendors.  - Incident response is seamless, with near–real-time data sharing across all stakeholders. |
| **Process** | - Every major or minor incident triggers formal updates; continuous improvement is embedded culturally.  - Security extends into supply chain, partner networks, and product/service lifecycle. | - Threat intelligence is shared proactively across partners and supply chains.  - Comprehensive tabletop exercises or red/purple teams validate readiness across multiple stakeholders.  - Minimal time from “discovery” to “corrective action” in any workflow. |
| **Technology** | - Fully orchestrated environment with dynamic adjustments, AI-driven insights, or advanced automation.  - Security architecture is continuously adapted to shifting risks and business objectives. | - Extended or integrated monitoring with real-time updates that keep coverage thorough and consistent.  - New features, vendor releases, or external solutions are rapidly piloted and adopted if beneficial.  - Rarely do threats go undetected for extended periods. |
| **Business Value** | **Transformative**  Security is not only controlling risk but actively enabling new market opportunities and innovation. Residual risk remains consistently below or equal to target thresholds. |  |

## Determining the Overall Stage Value

In many organizations, each of the four domains—Business, People, Process, and Technology—can evolve differently, creating challenges when summarizing the cybersecurity investment under a single IMPACTO stage. While approaches like the Lowest-Domain, Weighted-Average, or Tiered-Threshold methods exist, the **Recommended Two-Step Method** offers a practical balance between accuracy and motivation. Here is how it works:

1. **Set the Baseline at the Lowest Domain**
2. First, identify which domain (Business, People, Process, or Technology) currently holds the lowest maturity rating. That rating becomes the baseline, ensuring genuine limitations in critical areas are not overlooked.
3. **Determine if a One-Stage Bump Is Justified**
4. If at least two other domains are two or more stages higher than the baseline—and if a concrete, near-term plan (with timelines and budget) is in place to remediate the lagging domain—then raise your overall stage by one. This one-stage bump recognizes strong performance elsewhere while demanding real commitments to close the identified gap.

By applying these two steps, leadership can confidently communicate a single stage that reflects present constraints without undercutting progress in higher-performing domains. The method also drives a clear action plan for addressing shortfalls, helping teams track precisely what must happen for the overall stage to move up again.

Briefly, other methods may be used if an organization has specific needs:

* **Lowest-Domain**: Quick to implement, but can discourage teams that excel in multiple domains.
* **Weighted-Average**: Balances differences, yet risks hiding a weak domain behind high-performing ones.
* **Tiered-Threshold**: A hybrid that can slightly elevate the final rating if most domains are mature.

However, the **Recommended Two-Step Method** best aligns with IMPACTO’s principle of clear, data-driven improvement. It ensures that your overall stage value remains grounded in reality, highlights immediate remediation priorities, and rewards genuine leadership when multiple domains are demonstrably more advanced.

# Classification Frameworks

Organizations may ask how to align their existing cybersecurity frameworks with the IMPACTO Model’s post-purchase focus. Two classification frameworks—MCF (Maturity Classification Framework) and CCF (Capability Classification Framework)—help answer that question. MCF measures how well people and processes function consistently and repeatably, while CCF assesses how deeply a product’s features and integrations are utilized. By combining them, teams gain a complete picture of operational maturity and technical coverage, ensuring each investment drives meaningful risk reduction and business value.

## Maturity Classification Framework (MCF)

MCF evaluates the **Business, People, and Process** dimensions of an investment. Each domain’s maturity can be mapped to recognized standards like **NIST CSF**, **C2M2**, **SOC-CMM**, **Zero Trust** (CISA ZTMM), or **M3TID**, reflecting how systematically processes are governed and improved. For example:

* **Governance & Leadership**: Have roles, responsibilities, and escalation paths been formally established?
* **Process Consistency**: Do documented runbooks exist for major cybersecurity tasks, and are they updated regularly?
* **Metrics & Feedback Loops**: Are key performance indicators—like mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR)—tracked and used to refine incident response?

Many organizations mix multiple maturity models (e.g., SOC-CMM plus a Zero Trust framework) to create a single MCF that addresses unique business needs. Once defined, the MCF anchors the People and Process aspects of the IMPACTO Model, clarifying exactly which tasks, roles, and improvements are needed to move from ad hoc to fully optimized practices.

## Capability Classification Framework (CCF)

CCF measures how thoroughly the **Technology** side of a cybersecurity product is deployed. Mapping each feature to **MITRE ATT&CK** or **MITRE D3FEND** highlights which threats and defensive mechanisms are covered. Additional references—like **Essential Eight** or **Zero Trust**—help confirm that advanced features (e.g., micro-segmentation, machine learning) are in use rather than sitting idle.

To apply CCF:

1. **Inventory Capabilities**: Translate the Purchased Capability Profile (PCP) into a list of features you plan to enable.
2. **Map to Relevant Frameworks**: Link each feature to recognized threat or control frameworks (e.g., ATT&CK TTP coverage).
3. **Assign Stages (0–5)**: Align each feature with IMPACTO’s lifecycle, from “Purchased” (but unused) up to “Optimizing.”
4. **Review & Update**: Regularly verify coverage. If staff or processes lag, a high CCF rating can’t reduce risk alone.

## Integrating MCF and CCF

A core insight of IMPACTO is that neither mature processes (MCF) nor advanced product features (CCF) suffice by themselves. Both must progress in tandem. Highly trained teams accomplish little if their tools are only partially enabled, and a cutting-edge solution offers limited value if people lack the knowledge to operate it effectively.

For example, an enterprise invests in an advanced EDR platform (high CCF potential), but their runbooks are ad hoc and no one has been trained to interpret the new alerts (low MCF). Incidents slip through, and the tool’s full capabilities remain untapped.

Because IMPACTO focuses on optimizing cybersecurity investments post-purchase, it is beneficial to see how each IMPACTO stage (0–5) generally aligns with widely adopted frameworks:

| **IMPACTO Stage** | **NIST CSF Tier** | **C2M2 MIL** | **SOC-CMM** | **CISA ZTMM 2.0** |
| --- | --- | --- | --- | --- |
| **0 – Purchased** | Tier 1 | MIL0 | Ad Hoc | Traditional |
| **1 – Ad Hoc** | Tier 1 | MIL1 | Ad Hoc | Traditional |
| **2 – Managed** | Tier 2 | MIL2 | Managed | Initial |
| **3 – Formalized** | Tier 3 | MIL3 | Defined | Advanced |
| **4 – Data-Driven** | Tier 3–4 | MIL3+ | Quantitatively Managed | Advanced |
| **5 – Optimizing** | Tier 4 | MIL3+ | Optimizing | Optimal |

This chart is approximate rather than absolute. Nonetheless, it helps organizations familiar with one or more models (e.g., C2M2 or NIST CSF) see how to transition into IMPACTO’s more granular, post-purchase stages.

## Unified Assessments

For teams that already use M3TID, SOC-CMM, or other frameworks, combining them with MCF/CCF fosters a **unified assessment**. Doing so reveals whether:

* People and processes (MCF) keep pace with your tool’s **potential** (CCF).
* Technology gaps remain despite high process maturity.
* Certain threat tactics (from **ATT&CK**) remain uncovered or untested in real incidents.

This unified approach also supports continuous improvement. For instance, **Stage 4 (Data-Driven)** in IMPACTO aligns nicely with advanced threat intelligence in M3TID and thorough coverage in D3FEND.

The bottom line isMCF and CCF, guided by recognized standards (e.g., NIST CSF, C2M2, Zero Trust), let organizations track both procedural maturity and technical deployment. Each domain’s progress directly informs the overall IMPACTO stage, ensuring that investments are measured, optimized, and understood in the broader context of strategic cybersecurity goals.

# Capability Profiles

IMPACTO recognizes that real-world outcomes rarely match procurement-time assumptions. Two complementary profiles—Purchased Capability Profile (PCP) and Actual Capability Profile (ACP)—clarify this gap and drive each investment from untapped potential to consistent, measurable value.

## Purchased Capability Profile (PCP)

The PCP captures all the product features, technical functionalities, and integrations the organization *plans* to deploy. Drafted before or immediately after purchase, it acts as the roadmap for how the technology should ideally fit into the environment, including:

* **Key Features**: Which modules (e.g., advanced analytics, automated response) the organization intends to activate?
* **Integrations**: For optimal performance, external data feeds (e.g., threat intel) or services (e.g., identity management) are required.
* **Configurations**: Baseline “golden” settings—like correlation rules, alert thresholds, or custom dashboards.
* **Staff & Training**: Roles (e.g., SOC Analyst, Threat Hunter) required to operate the tool effectively, along with any needed training or certification paths.

A precise PCP aligns the investment with known threats, risk goals (PRP), and the operating environment (POC). Determining what the organization aims to achieve with each feature and outlining how each will be deployed significantly reduces the risk of leaving valuable capabilities unused.

Steps for Defining the PCP:

**Inventory Potential Features**

1. List relevant modules or functions and rate each by risk impact or compliance necessity.

**Align with Threat Scenarios**

1. Reference MITRE ATT&CK, D3FEND, or other frameworks to confirm which TTPs each feature addresses.

**Map Dependencies**

1. Note required log sources, data flows, external APIs, or integrations—plus any staffing or training prerequisites.

**Prioritize & Document**

1. For each feature, specify the success metrics (e.g., “reduce dwell time by 30%”) and identify the owner or champion.

## Actual Capability Profile (ACP)

While the PCP outlines intended capabilities, the ACP reflects how those capabilities function once deployed. It highlights which features are active, how well they work, and any variations from the original plan. The ACP is a living document, continuously updated as the environment (AOC) evolves and new insights (OI) emerge.

Even with a solid PCP, real-world constraints (e.g., misconfigurations and staffing gaps) can lead to partial or suboptimal usage. The ACP forces the organization to assess whether each feature fulfills its intended risk reduction, prompting timely adjustments that align the organization to its risk and maturity targets (PRP→ARP).

Steps for Defining & Refining the ACP:

1. **Deploy in Phases**

Follow a milestone roadmap that unlocks capabilities in smaller, manageable steps—verifying that each milestone aligns with the PCP.

1. **Pilot & Test**

Conduct proof-of-concept trials or test-lab scenarios to validate configurations; adjust the PCP if significant issues arise (e.g., high false positives).

1. **Collect Baseline Metrics**

Track mean-time-to-detect, mean-time-to-respond, and coverage of known TTPs to measure actual performance against PCP goals.

1. **Perform Gap Analysis**

Compare what is enabled (ACP) to the original PCP. Investigate root causes for any shortfall, such as insufficient training or missing integrations.

1. **Iterate Using Operational Intelligence (OI)**

Use incident data, threat intelligence, or tabletop exercises to identify missed detections or inefficiencies. Update rules, runbooks, or staff training as needed.

1. **Refresh Regularly**

Revisit the ACP whenever new staff join, significant incidents or environmental changes (AOC) arise. Over time, these incremental updates drive the overall maturity and risk posture forward.

# Operating Context

The Operating Context establishes a clear and structured view of where and how cybersecurity investments are intended to function within the organization. Applying consistent definitions from the C2M2 model—Enterprise, Organization, Function, and Architecture—helps frame the environments where security solutions operate, enabling precise management of risk, capabilities, and operational performance throughout the IMPACTO stages.

## Purchased Operating Context (POC)

The Purchased Operating Context (POC) is your initial strategic blueprint outlining where and how a cybersecurity investment will integrate into your environment. The POC leverages C2M2 definitions to address the following four layers systematically:

1. **Enterprise**: Clearly define the overarching organizational entity initiating and sponsoring the cybersecurity investment. This aligns with the highest-level decision-making body, influencing budget approvals and strategic risk alignment.
2. **Organization**: Specify the business units, subsidiaries, or departments directly involved in deploying and using the cybersecurity investment. Clarifying these entities ensures accountability and streamlined resource allocation.
3. **Function**: Outline precisely the operational scope—such as incident response, threat detection, and vulnerability management—that the purchased solution aims to enhance or enable. This ensures that operational objectives align explicitly with intended cybersecurity improvements.
4. **Architecture**: Detail the key technological structures, integrations, and data flows critical for the cybersecurity solution's intended capabilities. Mapping data ingestion points, log sources, platform integrations, and architecture dependencies ensure realistic deployment expectations.

Additionally, the POC should document essential assumptions regarding staffing requirements, training plans, initial configuration expectations (forming the Purchased Capability Profile, PCP), and risk-reduction targets (forming the Purchased Risk Profile, PRP). These assumptions establish a shared baseline, enabling consistent measurement of future performance.

**Practical Application**:

* To develop the POC collectively, hold collaborative workshops involving cybersecurity, IT, business leadership, and risk management teams.
* Document baseline assumptions about risks, intended capabilities, and operational processes, ensuring alignment with organizational strategies and budgets.
* To refine expectations, validate initial assumptions through scenario planning, tabletop exercises, or third-party expert reviews.

## Actual Operating Context (AOC)

The Actual Operating Context (AOC) captures real-world conditions, ensuring ongoing alignment between your cybersecurity solution and evolving business, technical, and threat environments. Over time, actual conditions inevitably differ from initial assumptions. The AOC systematically monitors these changes at all four C2M2-defined layers, enabling proactive management and alignment adjustments:

1. **Enterprise-Level Adjustments**: Document any shifts in executive sponsorship, changes due to mergers or acquisitions, or strategic realignments affecting the original enterprise assumptions.
2. **Organizational Changes**: Track evolving departmental structures, new reporting lines, or shifts in resource allocation that may impact solution ownership, operations, or budget responsibilities.
3. **Functional Adaptations**: Update the documented operational use cases and workflows as the security team's roles expand or shift to address new threats, compliance mandates, or business demands.
4. **Architectural Realities**: Regularly audit the technology landscape, capturing any new integrations, migrated platforms, changed data sources, or updated configurations. Identify gaps between actual deployment and original plans (PCP), prompting adjustments to close capability gaps.

Regular comparison between the POC and AOC reveals where deviations have occurred. Insights derived from Operational Intelligence (OI), threat assessments, and incident analyses help ensure your cybersecurity solution maintains maximum efficacy, delivering risk reduction (Actual Risk Profile, ARP) and actualized capabilities (Actual Capability Profile, ACP) closely aligned with the original intent.

**Practical Application**:

* Schedule regular cross-functional review meetings (monthly or quarterly) to systematically evaluate changes in the operational context, validate alignment, and document deviations from the original POC.
* Use gap analyses between PCP and ACP and between PRP and ARP to inform tactical adjustments—such as additional training, configuration tuning, or new integrations.
* Maintain a living document reflecting the current AOC, integrating it with Operational Intelligence to ensure the cybersecurity solution adapts swiftly and effectively to operational and threat landscape shifts.

By carefully defining the POC and consistently updating the AOC, the organization maintains a clear, shared understanding of how cybersecurity investments function in reality versus expectations. This structured approach supports ongoing optimization, aligns investments with strategic business objectives, and ensures cybersecurity continually delivers measurable, strategic value.

# Risk Profiles

Risk Profiles in the IMPACTO Model translate theoretical expectations (the **Purchased Risk Profile**, or PRP) into tangible, measured outcomes (the **Actual Risk Profile**, or ARP) using a **Risk Quantification Tool/Methodology** (RQT). This lets the organization track how a specific cybersecurity investment—and its corresponding capabilities—reduces residual risk over time.

## Purchased Risk Profile (PRP)

The PRP documents **how much** risk the organization expects to mitigate at the time of purchase. It highlights the threats the organization plans to address (e.g., ransomware, phishing, lateral movement) and the degree of risk reduction anticipated—often expressed in approximate Annualized Loss Expectancy (ALE-like) terms or simple High/Medium/Low ratings.

A clear PRP ensures executive sponsors, risk officers, and technical teams share the exact baseline expectations. This alignment reduces surprises if the Actual Risk Profile (ARP) later reveals unaddressed gaps.

Steps for Defining PRP:

1. **Identify Priority Threats**

List the top scenarios, referencing frameworks such as MITRE ATT&CK, D3FEND, or OpenCTI.

1. **Estimate Risk Reduction**

Use advanced modeling (e.g., FAIR) if you have robust data. Otherwise, approximate how much the organization expects to cut risk in more straightforward terms (e.g., 40% less chance of a breach).

1. **Document Preconditions**

Specify assumptions about staffing (e.g., dedicated SOC analysts) or process maturity (e.g., runbooks in place), ensuring the PRP remains realistic.

## Actual Risk Profile (ARP)

The ARP shows **what happens** once the solution is deployed, integrated, and operated in the real-world environment. It reflects whether the technology, people, and processes deliver the expected risk reduction from the PRP—or if gaps persist.

The ARP shows **what happens** once the solution is deployed, integrated, and operated in the real-world environment. It reflects whether the technology, people, and processes deliver the expected risk reduction from the PRP—or if gaps persist.

Steps for Defining/Refining ARP:

1. **Deploy and Measure**

Integrate logs, enable analytics, and track incident data (e.g., mean-time-to-detect/mean-time-to-respond).

1. **Compare PRP vs. ARP**

Identify whether the organization is meeting the expected risk reduction. For example, has the tool cut the chance of successful ransomware by 40%?

1. **Refine Continuously**

If shortfalls appear (e.g., missed detections, frequent false positives), revise your configurations, add staff training, or re-check the assumed threat coverage.

1. **Update Frequently**

Review the ARP as new threats arise, staff changes occur, or significant product features roll out. Real-time data (OI) helps you pivot quickly.

## Risk Quantification Tool/Methodology (RQT)

An RQT ensures consistent and transparent risk measurement at every stage (0–5). Novices can start with spreadsheet-based scoring from *How to Measure Anything in Cybersecurity Risk*, while advanced teams can leverage robust commercial tools. The **key** is maintaining the same approach over time so the PRP ↔ ARP comparisons remain credible.

**Choosing The Approach**

* **Lightweight / Spreadsheet**:
  + It is ideal if the organization lacks specialized staff or budgets.
  + Basic scoring (1–5) for likelihood and impact, or simple ALE-like formulas.
  + Good for early-stage (Stage 0–2) insights.
* **Advanced / Commercial**:
  + It suits organizations with deeper data, possibly in Stages 3–5.
  + May integrate continuous feeds from SIEM/EDR, real-time threat intel, or automated dashboards.
  + Supports scenario analysis, detailed ROI insights, or advanced model calibration (e.g., using FAIR).

This example demonstrates how to use risk quantification tools and methodologies—specifically RQT, PRP, and ARP—to assess a new Extended Detection and Response (XDR) solution aimed at reducing lateral movement risk.

1. **Identify the Investment’s Goals**
   * **Example**: Deploy a new XDR solution designed to reduce lateral movement risk by enhancing detection and response capabilities.
2. **Define the Purchased Risk Profile (PRP)**
   * **Set Expectations**: Clearly state the anticipated risk reduction (e.g., “Reduce successful lateral movement by 50%”).
   * **Document Assumptions**: Include prerequisites such as having a trained SOC analyst monitor and respond to XDR alerts, ensuring the expected risk mitigation is realistic.
3. **Deploy & Measure to Establish the Actual Risk Profile (ARP)**
   * **Integration & Monitoring**: Integrate XDR logs into the monitoring systems, actively track actual incidents, and record key metrics like mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).
   * **Comparison**: Assess whether the outcomes align with the initial PRP expectations.
4. **Quantify Risk Using an RQT**
   * **Basic Approach**: Estimate the annual frequency of lateral movement breaches and multiply by the estimated cost per incident.
   * **Advanced Approach**: Apply a framework such as FAIR or a robust commercial tool to simulate probabilities and quantify financial impacts more precisely.
5. **Close the Gaps**
   * **Identify Shortfalls**: If the ARP shows that the risk reduction falls short of the PRP, investigate potential causes—such as inadequate staff training, poorly configured alerts, or incomplete integration of critical features.
   * **Implement Improvements**: Address these issues with targeted actions, such as enhanced training, refined runbooks, or further technical tuning of the XDR solution.
6. **Iterate and Mature**
   * **Continuous Improvement**: Regularly update the ARP as the XDR configuration is refined and new threats emerge.
   * **Progress Tracking**: Over time, the risk posture should steadily move toward (and eventually exceed) the risk reduction goals set in the PRP, reflecting higher IMPACTO maturity stages.

This concrete example provides a clear roadmap for applying RQT, PRP, and ARP to a specific cybersecurity investment—ensuring that the XDR solution meets initial expectations and evolves through continuous measurement and improvement.

# Operational Intelligence

Operational Intelligence (OI) integrates real-world insights—including threat intelligence feeds, adversary research, incident reviews, and simulated attack exercises—into cybersecurity investments. This continuous integration ensures that the cybersecurity posture remains relevant, effective, and adaptable across every IMPACTO stage, transforming static investments into proactive defenses that evolve alongside the threat landscape.

**Why Operational Intelligence Matters in IMPACTO:**

1. **Bridging PRP to ARP:**

OI provides a critical feedback loop, refining the Actual Risk Profile (ARP) from the baseline assumptions set by your Purchased Risk Profile (PRP). Real-world incidents, simulation outcomes, and fresh intelligence reveal discrepancies, such as detection gaps or configuration oversights, allowing teams to adjust Actual Capability Profiles (ACP) to maintain alignment with risk-reduction objectives.

1. **Driving Domain Maturity:**

OI ensures that each maturity enhancement—whether updating runbooks, implementing new tools, or training personnel—addresses actual operational threats and gaps, not just theoretical risks. This targeted maturity advancement spans IMPACTO's Business, People, Process, and Technology domains.

1. **Enabling Data-Driven Progress:**

Rather than relying solely on periodic assessments, OI integrates continuous inputs from red and purple team exercises, post-incident analyses, and real-time threat intelligence. This proactive approach accelerates progression toward Stages 4 and 5, characterized by data-driven decision-making and real-time adaptation for optimal security effectiveness.

**Leveraging M3TID for Operational Intelligence:**

The M3TID (Measure, Maximize, and Mature Threat-Informed Defense) framework offers a structured approach to evaluate and enhance the effectiveness of OI:

* **Measure:** Assess the effectiveness of detection and response capabilities against adversary tactics (using frameworks like MITRE ATT&CK). Evaluate the speed and accuracy with which new threat intelligence is integrated into detection rules, runbooks, and training.
* **Maximize:** Focus on advancing the highest-risk scenarios by optimizing automated detection processes and specialized skill sets. M3TID identifies specific gaps, guiding resources to where they have the most significant impact.
* **Mature:** Continuously refine cybersecurity processes and technologies by incorporating simulation insights, incident analyses, and threat intelligence. This cyclical refinement is central to achieving and sustaining Stages 4 and 5 maturity levels.

By adopting M3TID principles, organizations objectively track their Operational Intelligence effectiveness, ensuring each intelligence input or incident review enhances real-world defense capabilities.

**Implementing Operational Intelligence for Cybersecurity Investments:**

1. **Identify Priority Threats:**
   * Utilize OSINT feeds, vendor advisories, and frameworks such as MITRE ATT&CK to identify adversary tactics, techniques, and procedures (TTPs) most relevant to the specific cybersecurity investment (e.g., EDR, cloud security, firewall).
2. **Establish OI Feeds and Testing:**
   * Integrate continuous threat intelligence feeds.
   * Schedule regular breach and attack simulations.
   * Institutionalize structured post-incident reviews to validate and enhance the logging, alerting, and automated responses.
3. **Compare Actual Outcomes to Expected Risk Reduction:**
   * Regularly measure whether your Actual Risk Profile (ARP) is moving toward your Purchased Risk Profile (PRP) objectives (e.g., a measurable decrease in successful attacks).
   * Investigate and remediate root causes if anticipated improvements fall short, such as training gaps or misconfigured tools.
4. **Iterate and Evolve Continuously:**
   * Update runbooks, refine alert thresholds, implement timely patches, and reinforce staff training as new threats and insights emerge.
   * Reassess effectiveness through recurring M3TID-driven exercises, confirming tangible risk reduction and progression through IMPACTO stages.
5. **Document and Share Findings:**
   * Maintain an up-to-date record of threat intelligence reports, detection logic changes, and outcomes of incident reviews.
   * Clearly link these operational insights to domain-specific maturity improvements—training enhancements in People, procedural updates in Processes, technical adjustments in Technology, and refined risk metrics in Business domains.

# Initial Momentum and Progressing Stages

Once a cybersecurity investment has been operationalized, the primary challenge is ensuring real progress beyond merely having a switched-on tool. Establishing **initial momentum** involves mapping actual usage to the Purchased Capability Profile (PCP) and aligning real-world outcomes with your Purchased Risk Profile (PRP). By continuously refining configurations and processes, the organization closes the gap between these purchased expectations and the Actual Capability Profile (ACP) and Actual Risk Profile (ARP). This early traction sets the tone for meaningful forward movement through the IMPACTO stages, preventing shelfware scenarios and building the confidence of executive sponsors. **Operational Intelligence (OI)** is a critical component for accelerating these gains, as mentioned in the preceding section.

## Operationalizing the Purchase Stage

In the early stages of a cybersecurity investment, it is not enough to purchase a tool or service. To move beyond mere acquisition and avoid the risk of "shelfware," the organization must actively plan and execute a series of decision-making steps that integrate the new asset into its overall security posture. This section introduces a detailed decision-making roadmap—illustrated by the flowchart below—that leverages key IMPACTO Model constructs, including the Purchased Capability Profile (PCP), Purchased Risk Profile (PRP), Projected Operating Context (POC), as well as the Maturity and Capability Classification Frameworks (MCF/CCF). The roadmap guides stakeholders through verifying business alignment, defining intended capabilities, establishing risk expectations, assigning responsibilities, developing processes, and executing an initial deployment. The steps are summarized below:

* **Step 1 - Verify Business Alignment & Define Risk Reduction Goal**  
  *Rationale:* Ensures that cybersecurity investment is justified through a clear return on investment (ROI) or risk reduction goal. Documenting the ROI prevents investments from remaining underutilized.
* **Step 2 - Define PCP & POC**  
  *Rationale:* By detailing the Purchased Capability Profile (PCP) and aligning it with the Projected Operating Context (POC), organizations ensure that the tool’s intended features are tailored to the real-world environment.
* **Step 3 - Establish the Purchased Risk Profile (PRP)**  
  *Rationale:* Setting risk targets through a formal risk quantification process establishes a baseline. This is critical for later comparing the Actual Risk Profile (ARP) to the PRP and measuring success.
* **Step 4 - Assign Roles & Responsibilities**  
  *Rationale:* Accountability is key. Assigning a product owner and ensuring proper training prevents the solution from becoming "shelfware" and builds the necessary human capacity to drive its use.
* **Step 5 - Develop Initial Processes**  
  *Rationale:* Establishing basic runbooks or Standard Operating Procedures (SOPs) moves operations from ad hoc to repeatable processes, setting the stage for a managed deployment.
* **Step 6 - Execute Initial Deployment**  
  *Rationale:* Operationalizing the solution (even if initially with default settings) is essential for realizing risk reduction. If the tool is not live, its intended benefits cannot be achieved.

A diagram of a flowchart

AI-generated content may be incorrect.

A diagram of a process

AI-generated content may be incorrect.

## Vendor and Professional Services Collaboration

Few organizations have all the expertise they need in-house; collaboration with vendors, professional service providers, and Value Added Resellers (VARs) can jumpstart or accelerate progress after the Purchase Stage. Product experts help tune essential features, align them with the environment, and identify advanced capabilities that often remain dormant. These partners also offer periodic “health checks,” ensuring that runbooks, detection logic, and integrations fully support your evolving risk posture. By coordinating goals, defining milestones, and regularly reviewing progress, the investment’s ability to deliver continuous value is safeguarded rather than stalling at a low maturity stage.

**External Roles and Their Contributions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Primary Focus** | **Typical Activities** | **Example Nexus** |
| Customer Success Managers (CSMs) | Adoption and value realization | Monitoring how well the purchased tool or service meets the organization’s risk-reduction goals (PRP);  Conducting “health checks” to review ongoing usage and flag underused features or integration gaps | Ensures the investment moves beyond shelfware (Stage 0–1) and actively contributes to higher maturity stages through structured feedback loops. |
| Technical Account Managers (TAMs) | Advanced configurations and technical integration | Orchestrating deep integrations across EDR, NGFW, SIEM, or SOAR platforms to narrow the gap between PCP and ACP;  Designing custom dashboards or analytics that feed into the organization’s risk quantification efforts (ARP) | TAMs often catalyze the shift from “Managed Deployment” (Stage 2) to “Formalized Integration/Data-Driven Solution” (Stage 3–4) by ensuring that features are configured optimally. |
| Vendor Support (Product/ Technical Support) | Ongoing maintenance and troubleshooting | Rapid patching and real-time remediation of product vulnerabilities;  Assisting during high-severity incidents to protect or restore critical capabilities, thus defending the intended ARP | Maintains operational continuity at any stage, preventing regressions that would keep the organization stuck at lower maturity levels. |
| Value Added Resellers (VARs) | Comprehensive solutions bundling, bridging capability gaps, and advisory. | Filling Roles or Services - A VAR might provide temporary SMEs (Subject Matter Experts) to handle EDR deployment or run NGFW health checks.  Bundling Solutions + Services - Offering a combined package (e.g., EDR tech + initial tabletop exercises), ensuring customers have the necessary tools and guidance. | VARs can streamline the transition between IMPACTO stages by quickly plugging skill or technology gaps, accelerating maturity across Business, People, Process, and Technology. |

## Visualization and Reporting

To maintain executive buy-in and user confidence, security improvements must be visible and quantifiable. **Journey Dashboards**—showing each domain’s (Business, People, Process, Technology) stage, risk metrics, and capability milestones—help everyone see precisely where they stand and what lies ahead. Overlaying baseline expectations (e.g., PRP, PCP) with Actual Profiles (ARP, ACP) underscores progress and clarifies any necessary course corrections.

**Risk & Cost Justification** reports, meanwhile, highlight tangible impacts on incident frequency, severity, and cost avoidance, reinforcing the value of ongoing program improvements. By linking changes in maturity and capability scores to real-world risk reductions, leadership can better evaluate where to invest next, ensuring each dollar spent produces a measurable return.

## Service Roadmap and AI-Assisted Planning

A **Service Roadmap** aligns quarterly or monthly initiatives—such as tabletop exercises, configuration reviews, and staff training—to desired maturity objectives. This timeline-driven plan prevents complacency by setting explicit milestones for each phase, ensuring the organization does not stall at a single stage.

The IMPACTO Model can also be encoded in **JSON schemas** to capture the Purchased Stage data (capabilities, expected risk, operating context) and automatically generate roadmap recommendations via AI-assisted tools. These schemas structure the data so that the following steps—like enabling specific advanced features or coordinating specialized training—can be quickly identified and scheduled. This streamlined, machine-readable approach helps the organization maintain a dynamic posture, adjusting swiftly as threats evolve or internal priorities shift.

# Key Terms and Acronyms

**Maturity & Capability**

**Maturity:**  
An assessment of how consistently cybersecurity processes (e.g., incident response, vulnerability management) are performed and improved within the organization. Evaluated using a structured framework (MCF) such as SOC-CMM or C2M2.

**Capability:**  
The technical features and functionalities of a cybersecurity solution, measured through a Capability Classification Framework (CCF) referencing standards like MITRE ATT&CK or MITRE D3FEND.

**Maturity Classification Framework (MCF):**  
Evaluates the consistency and continuous improvement of cybersecurity processes.

**Capability Classification Framework (CCF):**  
Measures the operational depth and effectiveness of cybersecurity technical capabilities.

**Profiles (Purchased vs. Actual)**

**Purchased Capability Profile (PCP):**  
A documented plan outlining intended technical features and capabilities of a cybersecurity solution at purchase.

**Actual Capability Profile (ACP):**  
The real-world capabilities achieved after deployment and configuration adjustments.

**Purchased Risk Profile (PRP):**  
The expected risk reduction and financial impact identified when acquiring a cybersecurity solution.

**Actual Risk Profile (ARP):**  
The measured and updated level of risk after deployment, refined through Operational Intelligence (OI) and actual performance data.

**Operating Context**

**Projected Operating Context (POC):**  
The planned environmental conditions (Enterprise, Organization, Function, Architecture) where the cybersecurity solution is expected to operate.

**Actual Operating Context (AOC):**  
The real-world operational environment, acknowledging changes post-deployment across Enterprise, Organization, Function, and Architecture dimensions.

**Risk Quantification & Intelligence**

**Risk Quantification Tool/Methodology (RQT):**  
Structured approaches (e.g., FAIR, NIST SP 800-30) used to quantify cybersecurity risks financially or numerically.

**Operational Intelligence (OI):**  
Insights derived continuously from threat intelligence, incident response, and operational data to refine cybersecurity practices.

**Program Optimization**

**Program Optimization:**  
The ongoing refinement of cybersecurity programs to enhance effectiveness, efficiency, and strategic alignment.

**Optimizing:**  
The highest IMPACTO stage (Stage 5), characterized by continuous adaptation, data-driven decision-making, and sustained strategic value.

**Domains & Stages**

**Domains:**  
The four IMPACTO focal areas—Business, People, Process, and Technology—that guide maturity and capability development.

**Stages:**  
The incremental maturity and capability milestones (Stages 0 to 5) defined within the IMPACTO Model.

**Performance Indicators & Metrics**

**ROI (Return on Investment):**  
The financial measure evaluating efficiency and effectiveness of a cybersecurity investment based on cost versus benefit.

**KPI (Key Performance Indicator):**  
Quantifiable metrics evaluating performance against defined cybersecurity operational goals.

**KRI (Key Risk Indicator):**  
Metrics indicating potential exposure to cybersecurity risks, enabling proactive response.

**MTTD (Mean Time to Detect):**  
The average duration to detect a cybersecurity threat or incident.

**MTTR (Mean Time to Respond):**  
The average duration required to respond to and remediate detected cybersecurity incidents.

**Frameworks & Methodologies**

**SOC-CMM (Security Operations Center - Capability Maturity Model):**  
Framework assessing and enhancing maturity in SOC processes and effectiveness.

**C2M2 (Cybersecurity Capability Maturity Model):**  
Framework developed by the U.S. Department of Energy for evaluating cybersecurity maturity levels.

**CISA ZTMM (Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model):**  
Structured approach to implementing and maturing Zero Trust security principles.

**NIST CSF (National Institute of Standards and Technology Cybersecurity Framework):**  
Cybersecurity best practices framework developed by NIST.

**NIST NICE (National Initiative for Cybersecurity Education):**  
Framework categorizing cybersecurity workforce roles, skills, and capabilities.

**MITRE ATT&CK:**  
Framework outlining adversary tactics, techniques, and procedures (TTPs) to guide cybersecurity defenses.

**MITRE D3FEND:**  
Framework cataloging defensive cybersecurity techniques and countermeasures.

**Risk Management & Intelligence**

**FAIR (Factor Analysis of Information Risk):**  
Methodology for quantifying cybersecurity risks in financial terms.

**ALE (Annualized Loss Expectancy):**  
The expected monetary loss from cybersecurity incidents over one year.

**M3TID (Measure, Maximize, Mature Threat-Informed Defense):**  
Framework guiding continuous improvement in threat-informed cybersecurity defenses.

**OSINT (Open Source Intelligence):**  
Information from publicly available sources used proactively to identify cybersecurity threats.

**Operational & Miscellaneous Terms**

**SOP (Standard Operating Procedure):**  
Detailed instructions for performing routine cybersecurity operations.

**VAR (Value Added Reseller):**  
Companies providing cybersecurity products enhanced by additional professional services.

**Shelfware:**  
Cybersecurity solutions purchased but underutilized or not deployed effectively.

**Health Check:**  
Routine evaluations ensuring cybersecurity solutions remain optimally configured and effective.

**Red/Purple Team:**  
Teams simulating cyber-attacks (Red) and collaborating defensively (Purple) to validate and improve cybersecurity defenses.

# References

**Australian Cyber Security Centre (ACSC).** (2023). *Essential Eight Maturity Model.* Australian Signals Directorate. Retrieved from https://www.cyber.gov.au/essential-eight/essential-eight-maturity-model

**Cybersecurity and Infrastructure Security Agency (CISA).** (2023). *Zero Trust Maturity Model (Version 2.0).* Retrieved from https://www.cisa.gov/sites/default/files/2023-04/zero\_trust\_maturity\_model\_v2\_508.pdf

**U.S. Department of Energy (DOE).** (2022). *Cybersecurity Capability Maturity Model (C2M2) Version 2.1.* Retrieved from https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

**European Union Agency for Cybersecurity (ENISA).** (2022). *ENISA CSIRT Maturity Framework.* Retrieved from https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework

**Hubbard, D. W., & Seiersen, R.** (2023). *How to Measure Anything in Cybersecurity Risk (2nd ed.).* Hoboken, NJ: Wiley.

**International Organization for Standardization (ISO/IEC).** (2022). *ISO/IEC 27005:2022 – Information security, cybersecurity, and privacy protection – Guidance on managing information security risks.* Geneva: ISO.

**MITRE Corporation.** (2020). *MITRE ATT&CK®: Design and Philosophy.* Retrieved from https://attack.mitre.org/docs/ATTACK\_Design\_and\_Philosophy\_March\_2020.pdf

**MITRE Engenuity.** (2023). *Measure, Maximize, and Mature Threat-Informed Defense (M3TID).* Retrieved from https://mitre-engenuity.org/cybersecurity/m3tid

**National Security Agency (NSA).** (2021). *NSA Funds Development, Release of D3FEND.* Retrieved from https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2665993/nsa-funds-development-release-of-d3fend/

**National Institute of Standards and Technology (NIST).** (2024). *NIST Cybersecurity Framework (CSF) 2.0.* (NIST Cybersecurity White Paper No. 29). Retrieved from https://doi.org/10.6028/NIST.CSWP.29

**National Institute of Standards and Technology (NIST).** (2020). *Workforce Framework for Cybersecurity (NICE Framework), Revision 1.* (NIST Special Publication 800-181). Retrieved from https://doi.org/10.6028/NIST.SP.800-181r1

**National Institute of Standards and Technology (NIST).** (2012). *Guide for Conducting Risk Assessments.* (NIST Special Publication 800-30 Rev.1). Retrieved from https://doi.org/10.6028/NIST.SP.800-30r1

**National Cyber Security Centre (NCSC).** (2023). *Cyber Security Investment: A Structured Approach.* Government Communications Security Bureau. Retrieved from https://www.ncsc.govt.nz/guidance/cyber-security-investment-a-structured-approach/

**OpenCTI Developers.** (2023). *Open Cyber Threat Intelligence Platform (OpenCTI).* Retrieved from https://opencti.io

**The Open Group.** (2021). *The Open Group Risk Analysis (O-RA) Standard, Version 2.0.1 (Open FAIR).* Retrieved from https://pubs.opengroup.org/security/o-ra

**van Os, R. M.** (2016). *SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers.* Luleå University of Technology. Retrieved from http://www.diva-portal.org/smash/get/diva2:1033727/FULLTEXT02.pdf

**Caralli, R. A., Allen, J. H., & White, D. W.** (2011). *CERT Resilience Management Model (CERT-RMM), Version 1.2.* Carnegie Mellon University. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9479

**SANS Institute.** (2023). *Incident Handler's Handbook.* Retrieved from https://www.sans.org/white-papers/incident-handlers-handbook/

**ISACA.** (2023). *COBIT Framework.* Retrieved from https://www.isaca.org/resources/cobit

**The FAIR Institute.** (2023). *Factor Analysis of Information Risk (FAIR).* Retrieved from https://www.fairinstitute.org/

**Cloud Security Alliance (CSA).** (2023). *Cloud Controls Matrix (CCM) Version 4.* Retrieved from https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

**OWASP.** (2023). *OWASP Top Ten Web Application Security Risks.* Retrieved from https://owasp.org/www-project-top-ten/

**Center for Internet Security (CIS).** (2023). *CIS Controls v8.* Retrieved from https://www.cisecurity.org/controls

© 2025 Kyle Villano – This document is part of the IMPACTO Model project and is licensed under the Creative Commons Attribution‑ShareAlike 4.0 International License (CC BY‑SA 4.0). To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/>