ACCELERATING BUSINESS OUTCOMES AND MANAGING OPERATIONAL RISK

Platform Overview

mitovia

About Us

- Cloud-based platform for capability and value management since 2011
- Clients in Utility, Transportation, Manufacturing, Public Sector, Consumer Goods, and other industries
- Extensive enterprise experience in cybersecurity, portfolio management, capability/process improvement, project delivery, and architecture management
- Published a book on “Achieving and Sustaining Secured Business Operations”
- Office and operations in USA and Canada
- Cloud-based platform and services hosted in Microsoft Azure data centers in USA and Canada

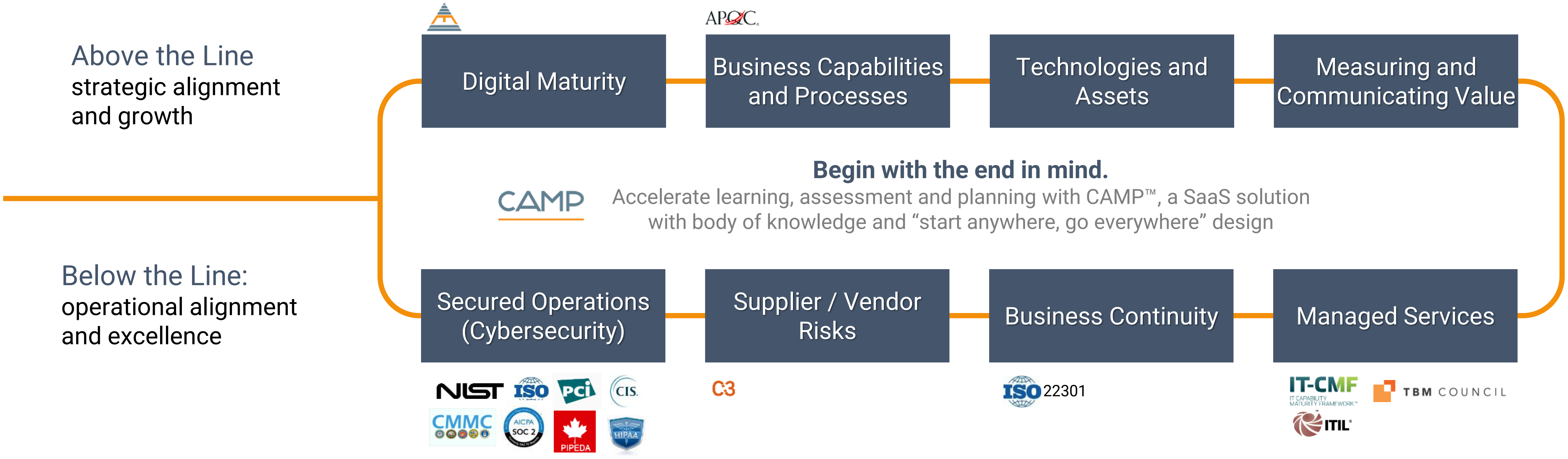
Mitovia
Philadelphia, USA

C3Plan
Toronto and Vancouver, CA

Our focus

Helping Organizations Achieve and Sustain Business & Technology Posture for Business Value, Organizational Capability and Operational Risk

at a fraction of the cost and time compared to the prevailing alternatives



Above the Line
strategic alignment and growth

Digital Maturity

Business Capabilities and Processes

Technologies and Assets

Measuring and Communicating Value

Begin with the end in mind.

Accelerate learning, assessment and planning with CAMP™, a SaaS solution with body of knowledge and "start anywhere, go everywhere" design

Below the Line:
operational alignment and excellence

Secured Operations (Cybersecurity)

Supplier / Vendor Risks

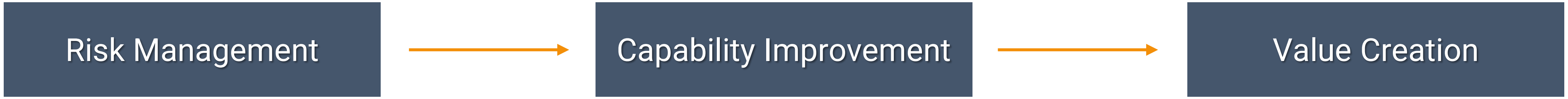
Business Continuity

Managed Services

Value Proposition

Risk-informed, Outcome-driven and Cost-effective Capability Planning by Operationalizing Knowledge and Actions

Improving organization's Business and Technology posture with



Risk Management

- Collecting and evaluating all relevant enterprise risks in one place
- Evaluating and addressing risks with purpose

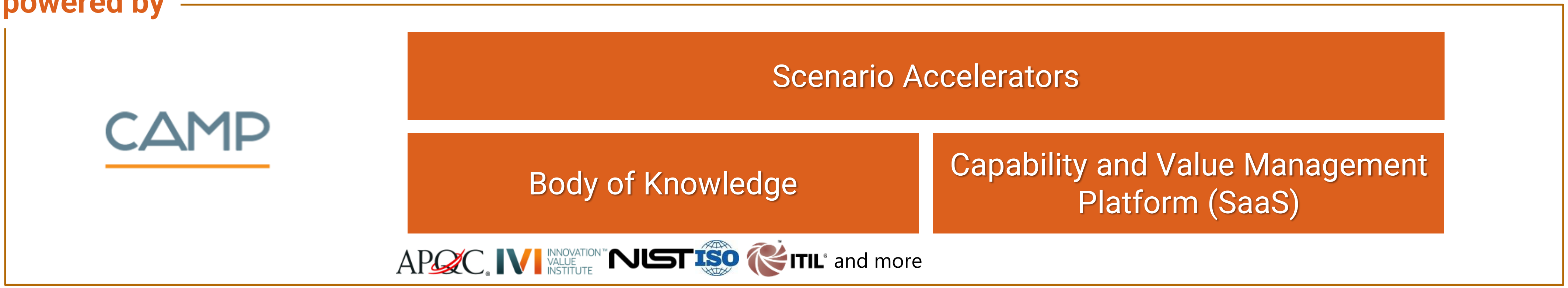
Capability Improvement

- Effectively assessing capability gaps against risks and business priorities
- Developing a prioritized, actionable roadmap

Value Creation

- Ensuring the improvement program is optimal
- Ensuring alignment and line of sight between initiatives and business value

powered by


CAMP
Scenario Accelerators
Body of Knowledge
Capability and Value Management Platform (SaaS)
APQC
IVI INNOVATION VALUE INSTITUTE
NIST
ISO
ITIL
and more

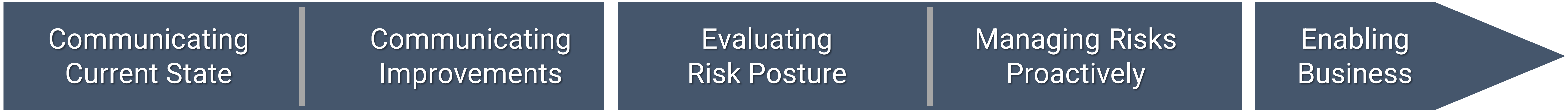
Assessing and Planning Cybersecurity with CAMP™

Helping organizations at different stages and accelerating improvement journey

1 Foundational
Understanding Capabilities

2 Operational
Managing Risks

3 Strategic
Creating Value



Communicating Current State

- State of cybersecurity practices using industry frameworks
- Multiple viewpoints
- Benchmarks
- Support audits

Communicating Improvements

- Year-over-year assessment and improvement reporting
- Improvement roadmaps
- Monitoring progress

Evaluating Risk Posture

- Risk register
- Risks-to-control mapping
- Plan practices and capabilities for priority risks

Managing Risks Proactively

- Periodical risk assessments
- Understand risks in applications and infrastructure
- Align investments and projects

Enabling Business

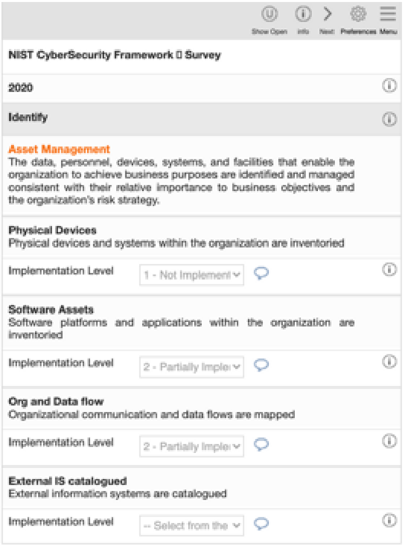
- Value flow maps
- Continuous risk management
- Optimize plans for business value
- Continuous improvement

CAMP ™ • End-to-End Lifecycle • Built-in Expert Knowledge • Agile • On-line, Authoritative Information

Cybersecurity Assessment and Planning Journey

03 Sample Artifacts

Configurable Questionnaire



NIST CyberSecurity Framework Survey

2020

Identify

Asset Management
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Physical Devices
Physical devices and systems within the organization are inventoried

Implementation Level: 1 - Not Implement

Software Assets
Software platforms and applications within the organization are inventoried

Implementation Level: 2 - Partially Imple

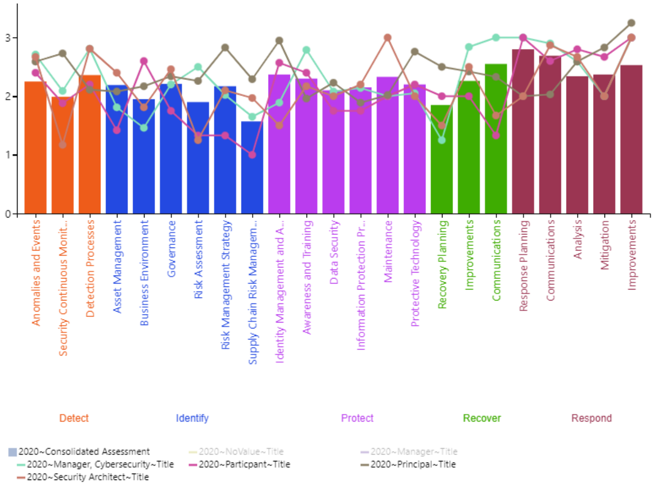
Org and Data flow
Organizational communication and data flows are mapped

Implementation Level: 2 - Partially Imple

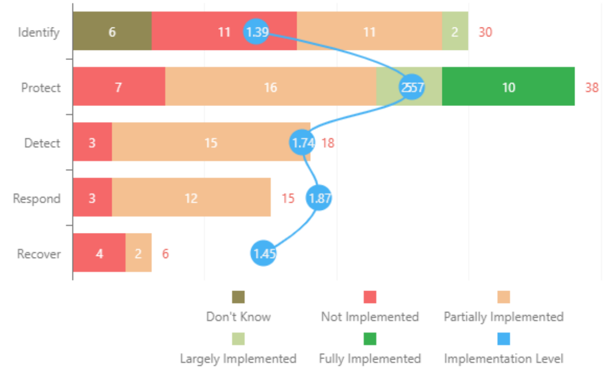
External IS catalogued
External information systems are catalogued

Implementation Level: -- Select from the

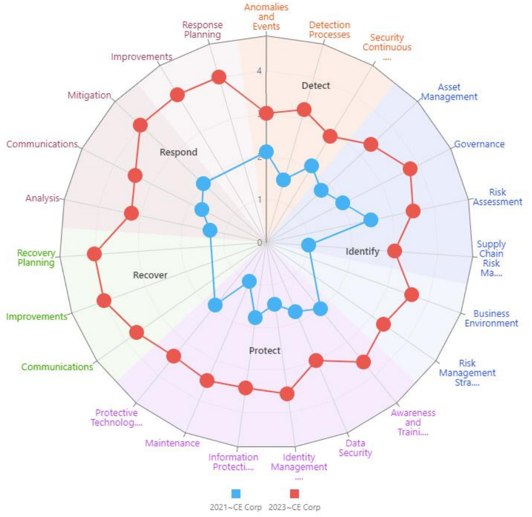
Segmentation Analysis, based on participants profile



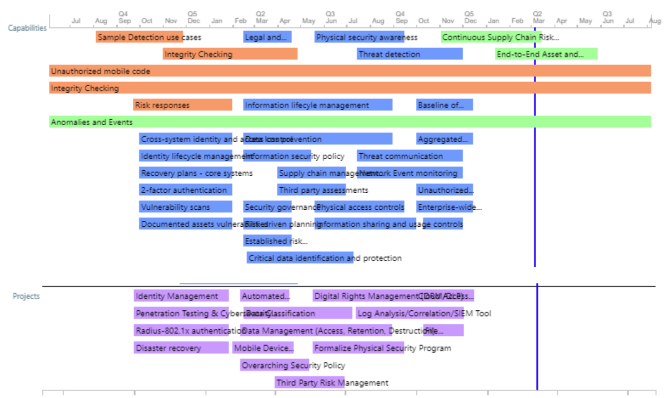
Maturity Distribution (level of readiness)



Year over Year Improvement

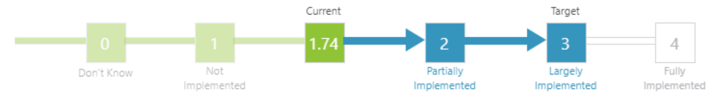


Roadmap from Recommendations



Recommendations to Close the Gap (leveraging body of knowledge)

Detect



1-Not Implemented --> 2-Partially Implemented

Recommended Areas of Improvement

Capability	Component	Description	Implementation Level
Security Continuous Monitoring	External service provider activity	External service provider activity is monitored to detect potential cybersecurity events	1.00
Detection Processes	Detection processes	Detection processes are tested	1.00
Detection Processes	continuously improve	Detection processes are continuously improved	1.00

Recommended Practices to Implement

Component	Scope	Practice	Description
continuously improve	Process	Detection methods	Ransomware attacks are continuously being refined, so detection processes must continuously evolve to keep up with new threats.
Detection processes	Process	Testing	Testing provides assurance of correct detection processes for ransomwarebased attacks, but not that all intrusion attempts will be detected.
External service provider activity	Technology	Monitor provider activity	Monitoring external service provider activity might detect ransomware events and other cybersecurity events before they have a chance to spread within the organization.

mitovia

Offerings: Helping Clients Succeed with CAMP

Replace current costly, time-consuming or ineffective methods e.g., using spreadsheets, consultants, or ad-hoc

Assessing and Planning Capabilities

- Evaluate current state of cybersecurity, supplier, business continuity, Cloud, Governance and DevOps capabilities and practices using industry frameworks
- Develop plan of action of close the gap
- Communicate current state and improvements over time

Potential Starter

Enable CISOs and CIOs to effectively manage their services for secured and reliable business operations

Managing Operational Risk

- Risk-driven approach to assessing and planning people, practices, and platforms (apps and infrastructure assets)
- Leverage and communicate using industry frameworks (NIST, ISO, etc.)
- Address cybersecurity, supply-side, business continuity, Cloud, Governance and DevOps

Value Offering

Support key initiatives e.g., cost reduction, M&A, ITSM/TBM, digital transformation etc.

Planning and Managing Strategic Value

- Organize and assess business and IT capabilities relevant to the initiative
- Model underpinning people, processes, information, technologies, and inter-dependencies
- Develop value flow maps and improvement plans
- Leverage and build upon many foundational components and body of knowledge

Initiative-driven