MāKINSIGHTS
Accomplish together

CRITICAL INDUSTRIES

Contents

- Introduction
- InfoSec Program HealthCheck
- Offensive Security
- Resiliency & Recovery
- Third-party Management – TPM
- ICS/OT Security
- Cyber Risk Quantification (based on FAIR)

Background

MAKINSIGHTS was founded in **2013 in Detroit, MI** and expanded to **Lima, Peru in 2018.** Our competitive edge is combining a global "Big-4" mindset with local talent and expertise through our worldwide footprint of partners and industry veterans possessing unique **INSIGHTS**

MAKINSIGHTS has successfully established programs and delivered innovative projects across **IT Risk Management, Privacy, Information Security, Cybersecurity,** and **IT Governance** in the US, Europe, Asia-Pacific, and South American countries

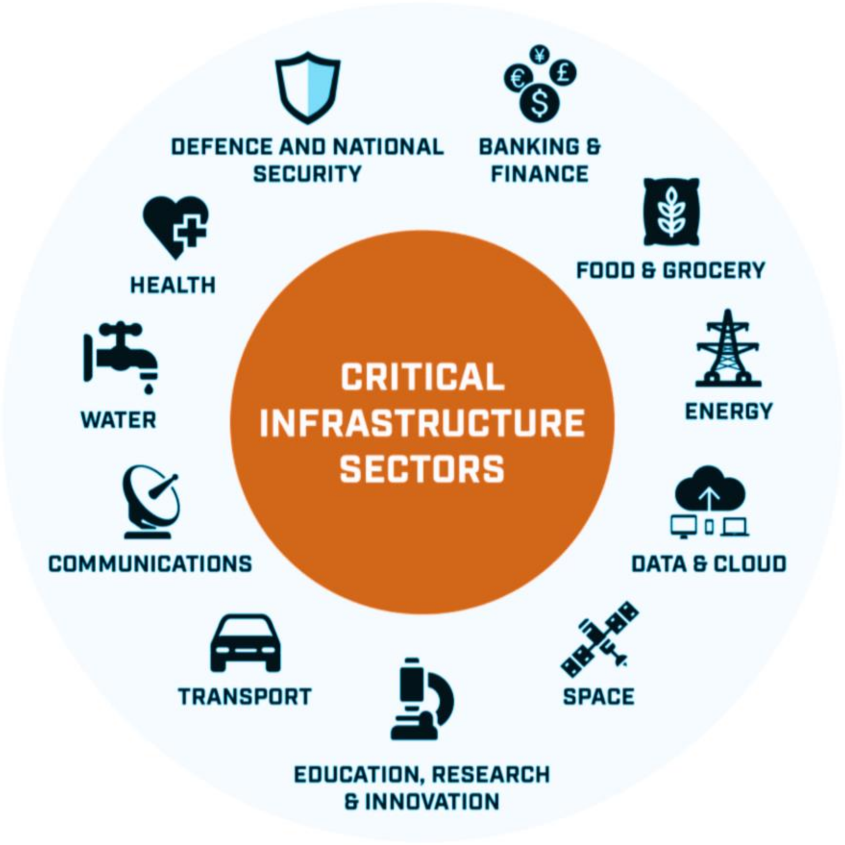
MAKINSIGHTS actively supports global organizations and those with other levels of scale in the following verticals:

- Manufacturing
- Financial Services
- Healthcare
- Internet/Technology
- Telecommunications & Utilities

Critical Industries Services Overview

Critical industries such as utilities, manufacturing, mining, and distribution have unique business demands that require a tailored Information Security strategy involving balanced aspects of governance, compliance, and technology investment to effectively support their mission.

MAKINSIGHTS offers an integrated set of advisory and service delivery capabilities to achieve this objective.


DEFENCE AND NATIONAL SECURITY
BANKING & FINANCE
HEALTH
FOOD & GROCERY
CRITICAL INFRASTRUCTURE SECTORS
WATER
ENERGY
COMMUNICATIONS
DATA & CLOUD
TRANSPORT
SPACE
EDUCATION, RESEARCH & INNOVATION

InfoSec Program HealthCheck

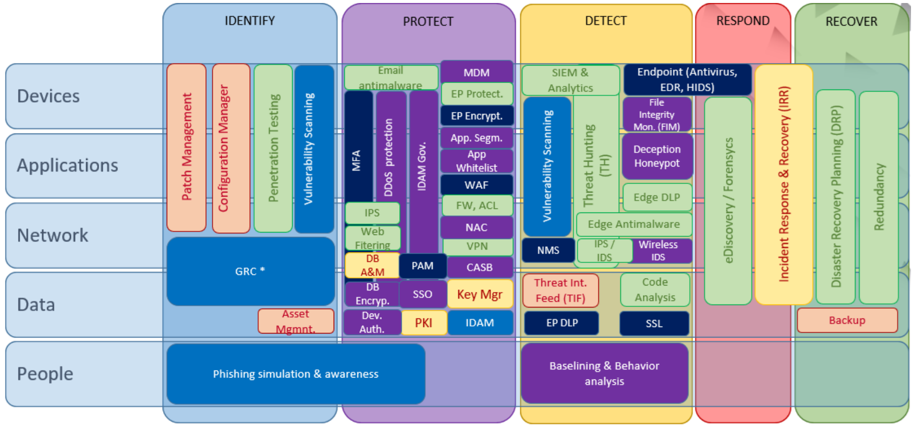
Obtain a 360-degree view of your Information Security, Risk, and Governance functions to understand your specific risks, strengths and weaknesses, while setting program priorities and validating the underlying investment roadmap

Benefits

- Understand your top risks and articulate how Information Security can best provide value to business partners
- Clearly align Information Security decisions with the Core Values and business strategy of the organization
- Establish a clear multi-year strategy supported by an investment roadmap
- Integrate internationally recognized principles and frameworks within the context of your program
- Simplify understanding of complex situations and develop messaging that resonates with the board and executive management

Typical activities

- Performing 360-degree meetings with LOB heads and executive management
- Reviewing governance decisions in the context of your business model
- Comparing your risk management approach against the 3-lines of defense paradigm
- Evaluating the convergence of the Information Security strategy with that of the broader organization
- Reviewing resiliency & incident response plans and conducting an abbreviated Top Risks workshop against Crown Jewels to better understand the potential financial impacts
- Conducting a maturity assessment against key standards such as ISO and NIST-CSF
- Tuning the Information Security strategy and investment roadmap to address key risks



Information Security Management
ISO 27001
Certified

Offensive Security

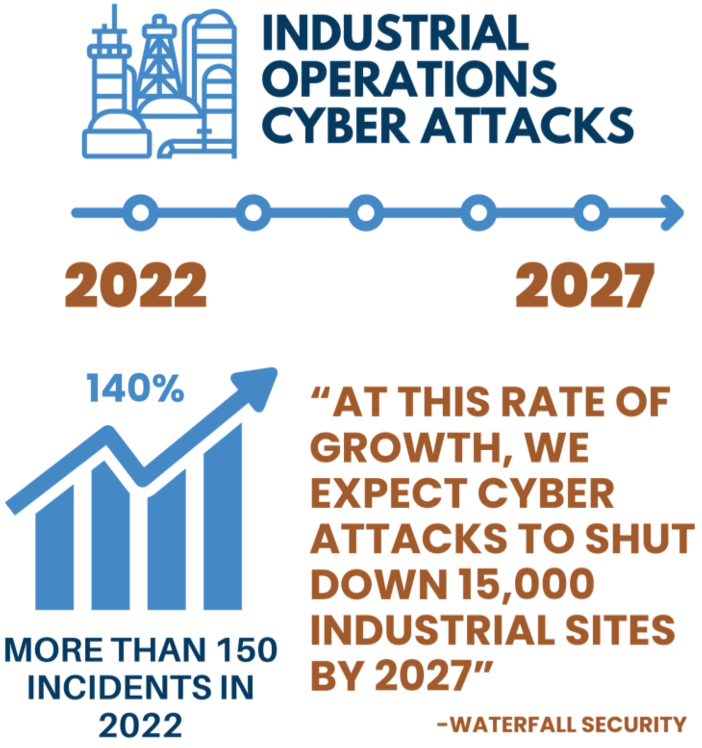
Proactively identify and address cyber weaknesses while being prepared to prevent, detect, and respond in a timely manner to focused threats that can impact the lifeblood of your business

Benefits

- Understand your true susceptibility to Ransomware and other Threats while prioritizing protection, detection, and response capabilities accordingly
- Promote fact-based engagement with important internal and external stakeholders such as the BOD, governance bodies, and regulators
- Promote cross-functional collaboration among IT, security, legal, communications, management teams and key suppliers
- Gain practical experience in dealing with attacks and decision-making under pressure
- Allow timely identification and correction of weaknesses prior to breach
- Ensure you can focus on protecting the right assets with the right set of controls at the right time

Typical service components

- Immediate Threat Analysis / Breach and Attack Simulation (BAAS)
- Penetration testing - Internal / External / Web & mobile
- Cloud-security reviews
- Security incident table-top exercises
- Ethical hacking, Red/Purple teaming
- Rogue/Trusted insider analysis



"AT THIS RATE OF GROWTH, WE EXPECT CYBER ATTACKS TO SHUT DOWN 15,000 INDUSTRIAL SITES BY 2027"

-WATERFALL SECURITY

Resiliency & Recovery

Ensure your organization is well-prepared to navigate significantly disruptive events and critical disaster scenarios in lock-step with the resiliency demands of your key business processes

Benefits

- Be prepared in the event of a disruption and reduce the potential negative impact on the organization
- Understand the needs of business partners and customers; translate these into a strategy composed of the specific capabilities needed by your program
- Align your organization’s resiliency strategy with the companies’ overall mission and goals
- Accurately link resiliency results to the strategic objectives of the business
- Understand the key business processes and their resiliency requirements
- Confirm and discover mission critical IT assets in your organization
- Allocate resources efficiently by identifying and prioritizing your most critical assets
- Leverage our expertise to quickly establish resiliency expectations and develop supporting services

Typical activities

- Identifying crown jewels and key processes of the organization
- Conducting a BIA (Business Impact Analysis) and risk analysis across people, process, and technology
- Developing the BCM (Business Continuity Management) strategy
- Creating enterprise guidance in the form of policies and standards
- Designing and establishing the business continuity plan and supporting procedures
- Testing the BCM plan using table-tops, simulations, and real exercises
- Providing feedback, training, and coaching to the internal team

Third-party Management - TPM

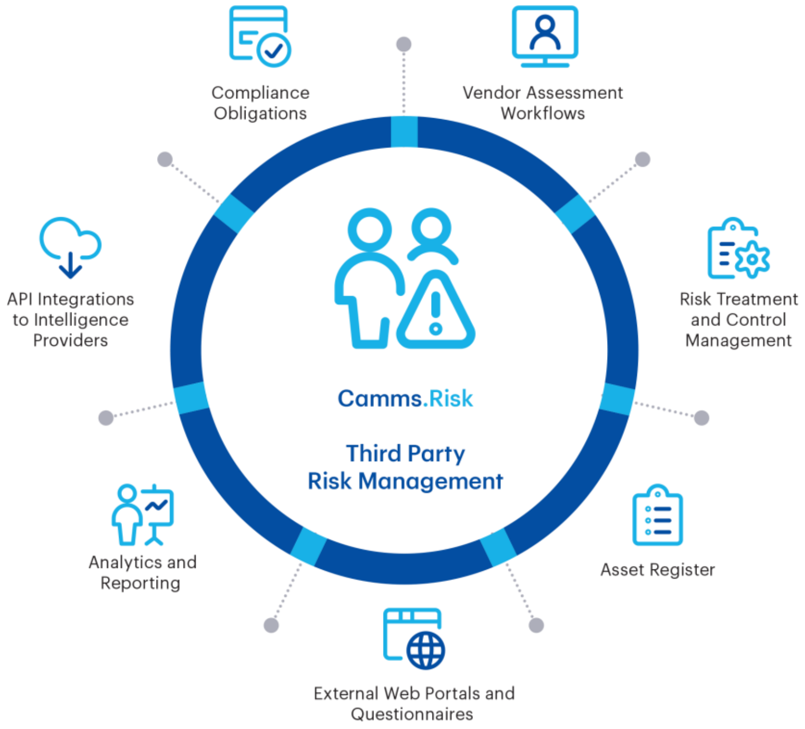
Improve the health of your supplier environment and ensure your organization is abreast of regulatory demands placed on the supply-chain through proactive management of third-party risk

Benefits

- Enhance the organization's capabilities to manage vendors
- Identify gaps in vendor Information Security capabilities and accelerate remediation
- Establish acceptable standards for managing vendors and contracts
- Implement an on-going monitoring capability that anticipates and assesses unforeseen risks
- Increased efficiency and cost savings across the vendor ecosystem

Typical activities

- Specifying acceptable contractual terms and conditions to protect your business
- Creating a governance program based on ITIL management principles
- Identifying essential and “risky” suppliers and classifying services by levels of criticality
- Designing, implementing, and maintaining governance programs for service providers
- Training of contract owners on third-party management expectations
- Providing ongoing support of “outsourced” vendor management programs


Compliance Obligations
Vendor Assessment Workflows
API Integrations to Intelligence Providers
Risk Treatment and Control Management
Camms.Risk
Third Party Risk Management
Analytics and Reporting
Asset Register
External Web Portals and Questionnaires

ICS/OT Security

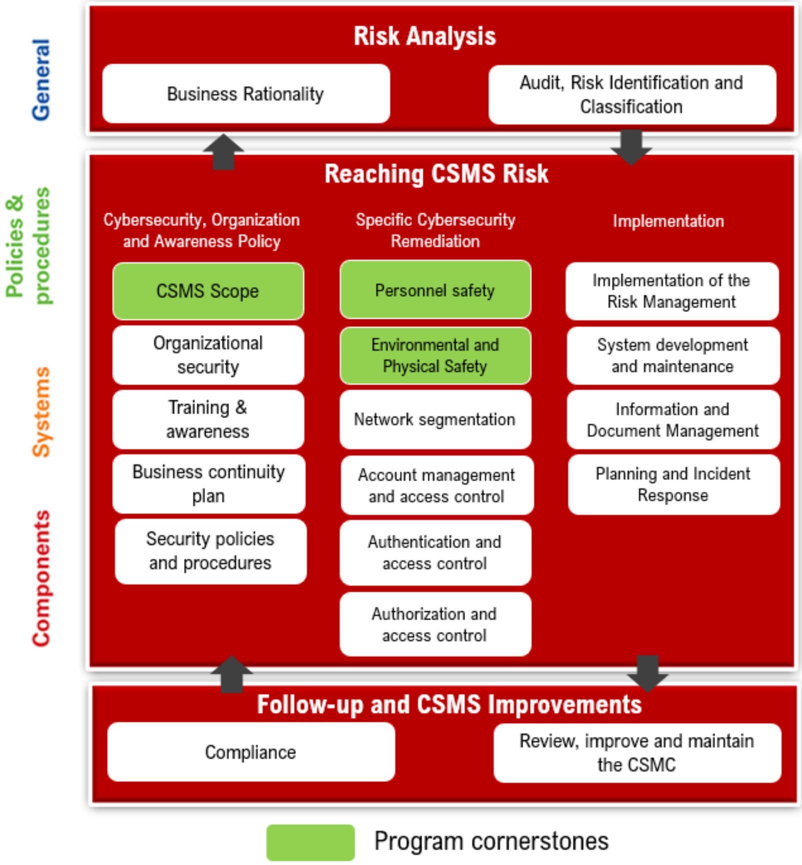
Implement an Industrial Cybersecurity Program converging your corporate and operational security strategy in alignment with many of the most important ICS/OT international standards such as ISA/IEC 62443 and ANSI/ISA99

Benefits

- Converge your Industrial Cybersecurity strategy with the corporate strategy
- Increase awareness of best practices for an Industrial Cybersecurity program and build partnership with Operations
- Leverage international standards & best practices to accelerate and support the development of your Industrial Cybersecurity program
- Understand the specific risks to your OT environment
- Provide appropriate levels of governance to ensure your Industrial Security decisions are aligned with your mission
- Protect your operational systems with the right set of investments

Typical activities

- Providing training and offering perspective to stakeholders on Industrial Cybersecurity Awareness
- Creating a programmatic governance model for Industrial Cybersecurity that supports the corporate vision and strategy
- Developing an asset inventory and defining system criticality; establishing a maturity baseline for the most critical operational systems
- Identifying key risks and developing a roadmap to prioritize remediation activities and supporting investments in people, process, and technology
- Engaging with executive management to secure the necessary budget and resources



General

Policies & procedures

Systems

Components

Risk Analysis

Business Rationality

Audit, Risk Identification and Classification

Reaching CSMS Risk

Cybersecurity, Organization and Awareness Policy	Specific Cybersecurity Remediation	Implementation
CSMS Scope	Personnel safety	Implementation of the Risk Management
Organizational security	Environmental and Physical Safety	System development and maintenance
Training & awareness	Network segmentation	Information and Document Management
Business continuity plan	Account management and access control	Planning and Incident Response
Security policies and procedures	Authentication and access control	
	Authorization and access control	

Follow-up and CSMS Improvements

Compliance

Review, improve and maintain the CSMC

🟩 Program cornerstones

Cyber Risk Quantification (based on FAIR)

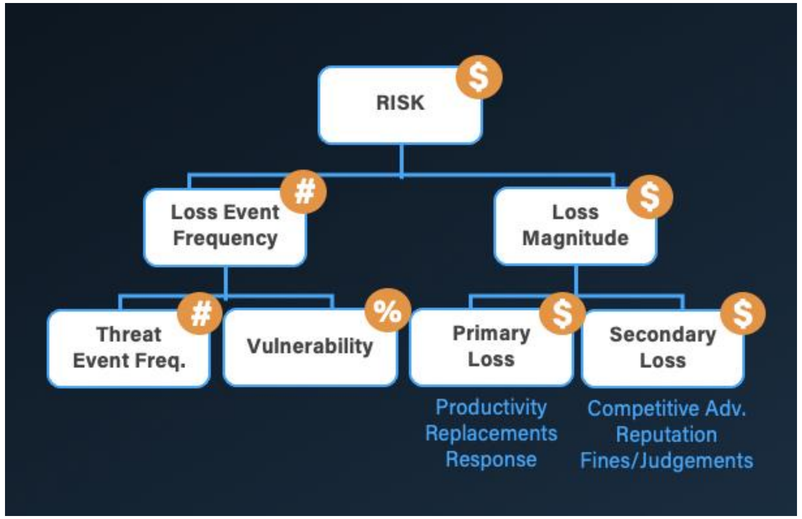
Quantify the financial implications of your organization's most important Information Security risks and develop Information Security messaging that resonate with the BOD and Executive Management

Benefits

- Understand your most critical information risks and ensure there are adequate treatment plans
- Effectively communicate information risks in financial terms with key decision makers such as the BOD, management team, senior executives, and other governance bodies
- Build a robust knowledge base that facilitates understanding the impact of critical risks on the business and improve investment decision-making overall
- Prioritize the most critical risk treatment options and make better investment decisions using limited funds
- Understand how different investments reduce your exposure to loss in financial terms and develop an optimal investment roadmap focused on management of information risk

Typical activities

- Training of personnel on the FAIR methodology
- Facilitating workshops and conducting interviews to understand key business processes and critical systems
- Collaboratively leading cross-functional working sessions to identify and quantify key risks
- Evaluating the impact of different controls on specific scenarios and in aggregate
- Adjusting and enhancing the Information Security strategy to drive financial reduction in risk
- Developing an optimized initiative roadmap to address risks
- Creation of materials for communicating to the BOD and Executive management
- Regular reporting of progress against plan and demonstrating how risk is being addressed in financial terms



Questions?

MāKINSIGHTS
Accomplish together

Management Team

Our team of seasoned professionals has led projects around the world for many of the largest and most recognized organizations, providing **MAKINSIGHTS** with deep domain expertise in **IT Strategy, Governance, Risk Management, Compliance, Privacy and Cybersecurity**

MARC KREVINGHAUS
MANAGING PRINCIPAL
President ISC2 - Peru

FELIPE CASTRO
Consulting Director

ANDRÉS AYBAR
Consulting Director

ANGEL LAY
Commercial Director

Contact Us

✉ ideas@makinsights.com

MAKINSIGHTS.com