InsightCyber IoT Risk Methodology™

InsightCyber managed IoT security services and risk assessments are based on industry best practices and the InsightCyber IoT maturity curve

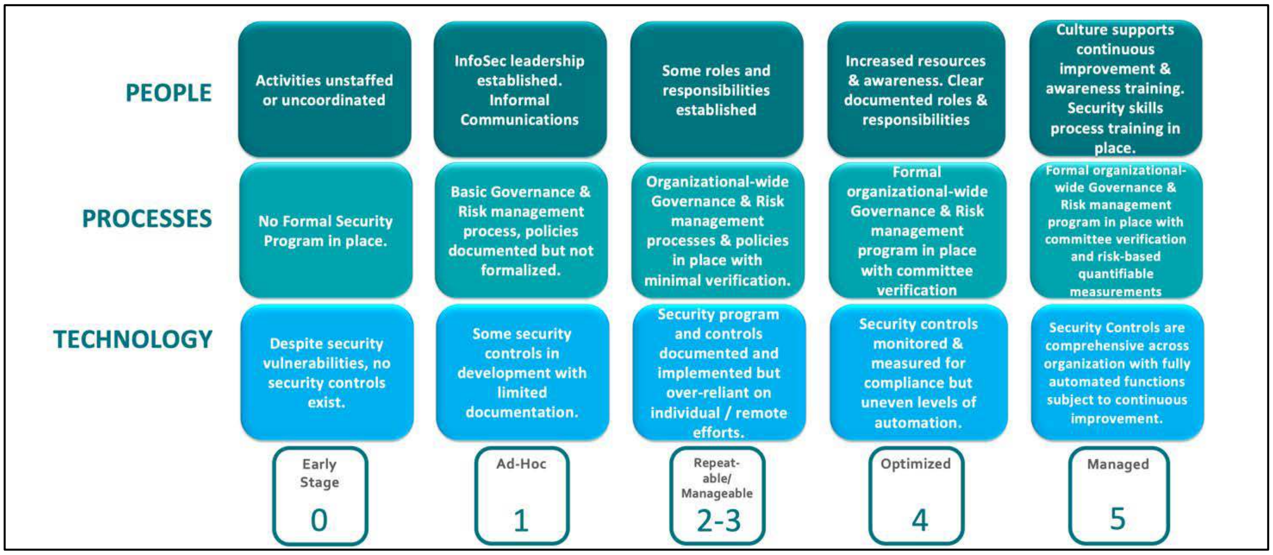
IoT cybersecurity is at the very beginning stages of its development. There are many ICS and IoT vendors, including many with household names, who are positioning themselves as the go-to player in the market.

To be truly effective, an IoT cybersecurity program must continually evolve and mature. The problem is, many ICS organizations don't have a clear sense of where they are today and how to improve for tomorrow. As Peter Drucker, the father of modern management, is often quoted as saying; "If you can't measure it, you can't improve it."

The IoT Maturity Model

To validate and measure IoT cybersecurity efforts, many rely on standard or known IT methodologies by counting vulnerabilities closed during a time period. Or they report compliance with a regulatory or industry standard. However, none of these approaches apply to IoT nor give a true indication of organizational maturity. Further, this does not provide a framework for IoT cybersecurity sustainability.

To measure, implement and improve on IoT cybersecurity, ICS organizations need to adopt a cybersecurity maturity model. At Insight Cyber Group, we have adopted a hybrid risk & maturity model to assess and rate IoT cybersecurity IoT cybersecurity.

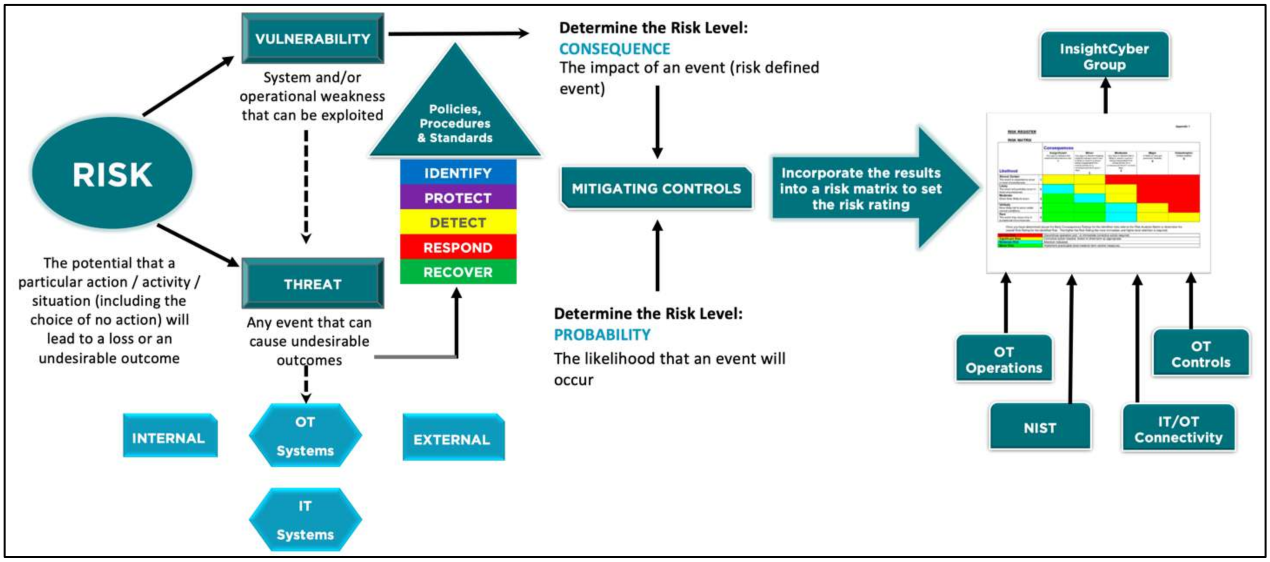


PEOPLE	Activities unstaffed or uncoordinated	InfoSec leadership established. Informal Communications	Some roles and responsibilities established	Increased resources & awareness. Clear documented roles & responsibilities	Culture supports continuous improvement & awareness training. Security skills process training in place.
PROCESSES	No Formal Security Program in place.	Basic Governance & Risk management process, policies documented but not formalized.	Organizational-wide Governance & Risk management processes & policies in place with minimal verification.	Formal organizational-wide Governance & Risk management program in place with committee verification	Formal organizational-wide Governance & Risk management program in place with committee verification and risk-based quantifiable measurements
TECHNOLOGY	Despite security vulnerabilities, no security controls exist.	Some security controls in development with limited documentation.	Security program and controls documented and implemented but over-reliant on individual / remote efforts.	Security controls monitored & measured for compliance but uneven levels of automation.	Security Controls are comprehensive across organization with fully automated functions subject to continuous improvement.
	Early Stage 0	Ad-Hoc 1	Repeat-able/ Manageable 2-3	Optimized 4	Managed 5

The InsightCyber IoT Security Maturity Model.

A cybersecurity maturity model provides a framework for measuring the maturity of a cybersecurity program and provides guidance on how to reach the desired level. There are several cybersecurity maturity models from which to choose. While we try to be as agnostic as possible, we have adopted the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) and the Department of Energy Cybersecurity Capability Maturity Model (C2M2) into our model. Both provide a comprehensive approach that covers everything cybersecurity.

The C2M2 was developed by the U.S. Department of Energy. However, we have adopted its use to measure the maturity of cybersecurity capabilities within IoT. The model consists of 10 Domains and provides a measurement for each, identifying areas of weakness, strength and status as it relates to Industry peers.


RISK
The potential that a particular action / activity / situation (including the choice of no action) will lead to a loss or an undesirable outcome
VULNERABILITY
System and/or operational weakness that can be exploited
THREAT
Any event that can cause undesirable outcomes
Policies, Procedures & Standards
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
INTERNAL
OT Systems
IT Systems
EXTERNAL
Determine the Risk Level:
CONSEQUENCE
The impact of an event (risk defined event)
MITIGATING CONTROLS
Determine the Risk Level:
PROBABILITY
The likelihood that an event will occur
Incorporate the results into a risk matrix to set the risk rating
InsightCyber Group
OT Operations
NIST
IT/OT Connectivity
OT Controls

The InsightCyber IoT Cyber Risk Methodology.

The NIST CSF differs from the C2M2 in that NIST CSF doesn’t consider CSF a maturity model. Instead of ten domains, the NIST CSF represents five cybersecurity functions. However, NIST CSF does denote a progression expressed as tiers. Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk informed. In other words, the tiers are an indication of the maturity level.

Our approach doesn’t stop there. With IoT cybersecurity we must also take into consideration the internal IoT Operations and IoT Controls. IoT Operations outline the “how” operations are done, and IoT Controls outline the “why.”

This is extremely important because not all cyber vulnerabilities operate in Layer 3 (Network), or Layer 4 (Transport), Layer 6 (Presentation) or Layer 7 (Application). IoT Operational/Control anomalies can lead to conditions that impact operations, business delivery, revenue & safety. Further, IoT Operational/Control anomalies can lead to a cyber event. In summary:

NIST CSF	→	Assesses against industry standards and best practices
M2C2	→	Assesses the capability & progression in a discipline
IoT OpCon	→	Assesses the ICS capabilities within the cyber domains and functions

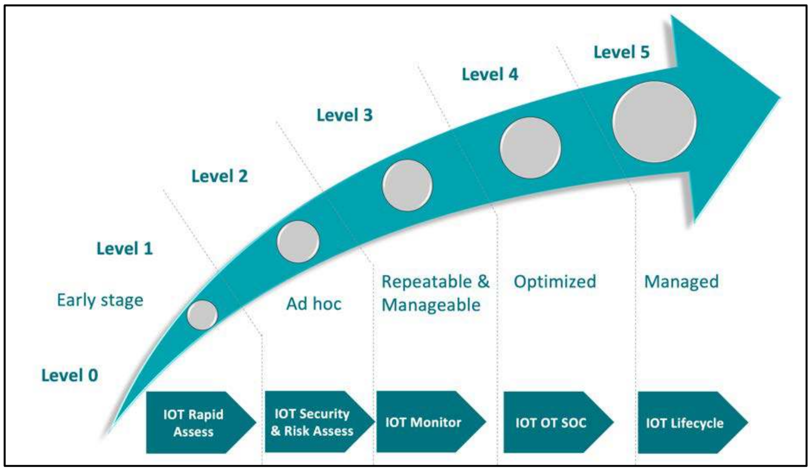
IoT Risk Methodology

The best of each of these approaches are combined in the InsightCyber Risk Methodology.

Our InsightCyber IoT risk assessments use an underlying risk methodology that focuses on specific controls that access critical assets, infrastructure, IoT controls, IoT operations and connectivity. We do this by reviewing the existing IoT posture. Our methodology also emphasizes operational best practices for each Control area, as well as the organizational effectiveness and maturity of internal policies and procedures.

There are three types of Risk Assessment performed by Insight Cyber Group depending upon where the ICS/OT organization is currently on the IoT Maturity Curve.

Insight Cyber Risk Methodology-Based Services



The InsightCyber IoT Risk Maturity Curve.

Rapid Assess

When an ICS organization is at the very beginning stages of understanding IoT cybersecurity, the IoT Rapid Assess service provides a short IoT Risk Assessment defined to discover what is happening within the ICS environment.

From an IT perspective, the IoT Rapid Assess is like an NMAP, but much more. The The IoT Rapid Assess service also provides fully actionable, context-enriched reporting, visualization and events. The service will tell you what assets you have, what they're doing, who is talking to whom, how they are communicating and whether they are vulnerable to cyber attacks. The IoT Rapid Assess service can also accurately detect rogue devices, unauthorized applications and services and cyber infiltrations that are already running in the ICS environment.

The results of the IoT Rapid Assess includes a highly technical report as well as a high-level overview of the status of the IoT cyber program. The IoT Rapid Assess is designed to allow the CISO to have actionable information to take to the Board for the development of a broader IoT cyber program.

Security & Risk Assess

At this phase of the curve, the ICS organization is at the point where executive by-in for developing an IoT cybersecurity program has been achieved. But where to start?

The InsightCyber Security & Risk Assess service is a comprehensive ICS cyber risk assessment. It takes the NIST CSF, C2M2 model and the InsightCyber risk methodology (IoT Operational/Controls) and assesses all aspects of an organization's ICS environment.

Security & Risk Assess is divided into four phases; 1) pre-assessment questionnaire, 2) onsite walk-thru and Interviews, 3) OT and IT network analysis scans and 4) gap analysis. The service aims to be as efficient as possible. We assess people, processes, controls, connectivity, technologies and safety conditions. We will get deep into the weeds and gauge the effectiveness of existing controls, cyber exposure, risks to operations, revenue and corporate impact.

IoT Lifecycle

At this stage, the ICS organization has achieved a high level of maturity. There is an established ICS cybersecurity program and risk management process in place. The board has established budget for the program. At this stage the question becomes "how valid is the cybersecurity ad risk program?"

The InsightCyber IoT Lifecycle service is a validation assessment. It is designed to assess the operational IoT cybersecurity & risk management operations and processes. Lifecycle Management is another term that is used in many contexts, but in general applies to managing the development, acquisition, implementation, use and disposition of an entity (in this case, that entity is IoT cybersecurity). With the IoT Lifecycle, we take a deep dive into the 'process of running and managing IoT cybersecurity activities.

The IoT lifecycle reviews the IoT cybersecurity program including: Implementation, Delivery, Success Factors, Knowledge & Awareness, Integration, and Effectiveness.

Note: There are two other InsightCyber services associated with the IoT Maturity Curve that do not incorporate the InsightCyber IoT Risk Methodology: These are IoT Monitor (phase 3) and OT SOC (phase 4). The IoT Monitor service provides 24x7x365 visibility and threat monitoring for an unlimited number of plants. OT SOC extends IoT Monitor with incident response, KPI monitoring and remediation capabilities.

About InsightCyber

Insight Cyber Group, Inc. provides a suite of advanced managed IoT security services through MSSPs and other partners. Our services deliver continuous, real-time monitoring, visibility, cyber-risk management and improved operational efficiencies for ICS/OT/IOT assets and cyber-physical systems.

Email: info@insightcybergroup.com | **Web:** www.insightcybergroup.com | **Social:** #InsightCyberIoT