Case Study

Genuine Parts Company Builds Cyber Resilience with ISACA’s CMMI® Cybermaturity Platform

The Business Need

Cybersecurity is the #1 corporate governance challenge today — yet 87% of C-Suite professionals and board members lack confidence in their company’s cybersecurity capabilities. 1 Genuine Parts Company, a multi-billion dollar, global service organization with over 55,000 employees, wanted better insight and management of their cybersecurity risk and complex security requirements to demonstrate their cyber resilience and mitigate cybersecurity risk. Genuine Parts wanted to align their cybersecurity processes and maturity along a common assessment framework.

They needed a powerful tool that could be readily customized, shared and tracked by their cybersecurity and compliance professionals. They also wanted to create a shared approach and framework to communicate with enterprise leaders. To accomplish this, Genuine Parts selected ISACA’s CMMI Cybermaturity Platform to conduct a cyber maturity self-assessment because it provided an evidence-based approach for assessing, optimizing and reporting on cyber capabilities and framework alignment, and was able to be completely customized for Genuine Parts’ unique requirements.

What is the CMMI Cybermaturity Platform?

The CMMI Cybermaturity Platform helps large enterprises manage enterprise cybersecurity resilience, readiness and board confidence, as cyber threats and security requirements continue to evolve. This first-ever cyber maturity platform provides enterprises with the evidence-based insights they need to mitigate cybersecurity risk and build cyber maturity. CISOs and CIOs can confidently measure, assess and report on cyber maturity across the enterprise, aligned with globally-accepted industry standards.
The cloud-hosted CMMI Cybermaturity Platform offers:

- **An industry-leading, enterprise-level solution** that can be administered in-house or by professional experts and tailored to the unique needs of your business
- **A risk-focused capability self-assessment** that targets the areas most relevant to your enterprise
- **A risk-prioritized roadmap** that helps you focus cyber investments on the threats that will have the greatest impact
- **Assessment findings that align with global, recognized standards**, including NIST (CSF, SP 800-171), ISO/IEC (27001, 27002), Threat Kill Cycle, FFIEC and CMMC

**The Business Challenge**

Genuine Parts Company determined that its initial cyber maturity assessment needed to create a baseline against a common framework that aligns with NIST CSF and the ISO 27001 controls. They needed to assess multiple units, demonstrate maturity that was aligned with the NIST CSF, and specifically focus on demonstrating maturity performance in managing risk, not something compliance-based. Genuine Parts customized the CMMI Cybermaturity Platform to target these specific areas for improvement in their assessment.

- Apply governance elements
- Apply risk strategy
- Implement risk management
- Implement risk identification
- Ensure access control management
- Apply data security protection
- Apply organizational training
- Ensure trustworthy systems
- Apply operational protection provisions
- Apply protection planning
- Apply protective technology provisions
- Apply cybersecurity incident detection
- Apply continuous monitoring
- Apply incident response
- Apply incident handling
- Apply incident recovery

“The CMMI Cybermaturity Platform has enabled us to establish a quantitative baseline measure for our security program maturity in a very cost effective manner. The ability to customize the solution to our specific risk profile was a key differentiator in our selection process.”

Damian Apone
Global Security Program Director
Genuine Parts Company
The Solution
The CMMI Cybermaturity Platform Enables Genuine Parts Company to Conduct an Actionable and Insightful Cyber Maturity Assessment

Genuine Parts selected the CMMI Cybermaturity Platform because of its alignment with globally recognized standards, particularly the NIST Cyber Security Framework (CSF), as it is already an industry benchmark with risk-based controls. Additionally, its Informative References and alignments across the 20 CIS (Center for Internet Security®) Cyber Security Controls, COBIT Controls, ISA–62443-2-1–2009 (Security for Industrial Automation and Control Systems), ISO/IEC 27001 INFOSEC Controls, and the federal controls NIST SP 800-53 Rev. 4 -1 provide additional utility. To succeed, Genuine Parts determined that their initial CMMI Cybermaturity Platform maturity assessment model be:

• Digital
• Risk-based
• Provide a risk profile/map
• Easy to use
• Customizable
• Self-paced
• Align to the NIST Cyber Security Framework (CSF)
• Align to the ISO 27001 Controls for ease of self-assessment and improvement
• Produce a roadmap for improvement

As Genuine Parts developed their customized risk profile, the descriptors for each frequency of occurrence values led to invaluable discussions among the Genuine Parts senior leaders. Without these definitions, calibrating their current state and then defining improvement goals would have been nearly impossible.

In addition, using the CMMI Cybermaturity Platform Maturity Scorecard within each Practice Area Assessment allowed employees to review and understand the People, Process, and Technology (PPT) objective for each maturity level, and its relative ISO 27001 Informative Reference by Maturity Level. This view provided specific insights for measured vs. targeted maturity levels—an eye-opening experience and a rallying cry for achieving continuous improvement.
Key Performance Goals Achieved

While the Genuine Parts Company Enterprise Security Team could not control the number of security incident tasks it received, it could control how it handled their resolution in a more efficient and timely manner. Since the CMMI Cybermaturity Platform self-assessment in January 2020, they have:

• Reduced Mean Time to Task Resolution (MTTR) from nearly 24 days (23.9) over the previous three quarters to an average of 6.5 days for the first two quarters in 2020
• Decreased the range of Backlog Days for Tasks from as high as 117 days during the previous three quarters, to a low of six days for the first two quarters in 2020

Addressing Improvement Opportunities

Genuine Parts Company is increasingly shifting to a risk-based approach to the use of controls and cybersecurity frameworks. This has changed its whole basis of reference when leaders speak to each other. In the past, leaders based their performance perceptions upon perceived internal and uncalibrated frameworks from former experiences. This would lead to biased and perhaps misaligned deployment with mixed results. Using the CMMI Cybermaturity Platform and its self-assessment feature, Genuine Parts now has a comprehensive, objective and usable roadmap that was validated by an additional 3rd party assessment.

Part of Genuine Parts Company’s 2018–2019 Strategic Planning Process was the adoption and alignment to the NIST Cyber Security Framework and its Five Functions of Identify, Detect, Protect, Respond, and Recover. C-Suite buy-in was much easier since the CMMI Cybermaturity Platform had the benefit of not just being grounded in the use of the CMMI model, but the added bonus of its alignment to the NIST Cyber Security Framework, its Five Functions, their Categories and Subcategories and Informed References throughout the Practice Area Assessments and reports.

The self-assessment feature offers a comprehensive, objective, and usable roadmap.
Lessons Learned

Prior to Genuine Parts Company's initial self-assessment using the platform, company leaders felt they were just spending money and making reactionary decisions for cybersecurity based upon preconceived, and often misaligned perceptions. Now, pulling from the NIST Cybersecurity Framework, its alignment to ISO 27001, Genuine Parts’ CMMI Cybermaturity Platform self-assessment and its validation by their 3rd party Cyber Maturity Assessment (CMA), Genuine Parts is now making risk-based cybersecurity decisions.

Verifying data and spending the time needed to accurately determine Incident Pattern Prioritization can be immensely valuable: Genuine Parts found that they previously set higher maturity targets for themselves than were warranted. This realization helped them recalibrate their Risk Profile for some Potential Events and Vulnerabilities. Based on the feedback from the CMMI Cybermaturity Platform self-assessment, Genuine Parts is now preparing to launch an improvement program for the identified improvement projects to realize the benefits of their respective cybersecurity maturation.

Learn more about the CMMI Cybermaturity Platform: www.isaca.org/cybermaturity

“Key items that led to our selection of the CMMI Cybermaturity Platform include the mapping to multiple frameworks (e.g. NIST, ISO, etc.), along with the ability to customize the evaluation to our specific risk profile. Additionally the remediation roadmap functionality has helped us to identify what specifically we need to do to improve our maturity as well as helps us in prioritizing the efforts.”

Damian Apone
Global Security Program Director
Genuine Parts Company

© 2021 ISACA. All rights reserved.

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organization that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide.

ISACA’s CMMI enables organizations to elevate and benchmark performance across a range of critical business capabilities, including product development, service excellence, workforce management, data management, supplier management, and cybersecurity. For more than 25 years, thousands of high-performing organizations have achieved sustainable business success through CMMI adoption and demonstrated their ability as capable business partners and suppliers.