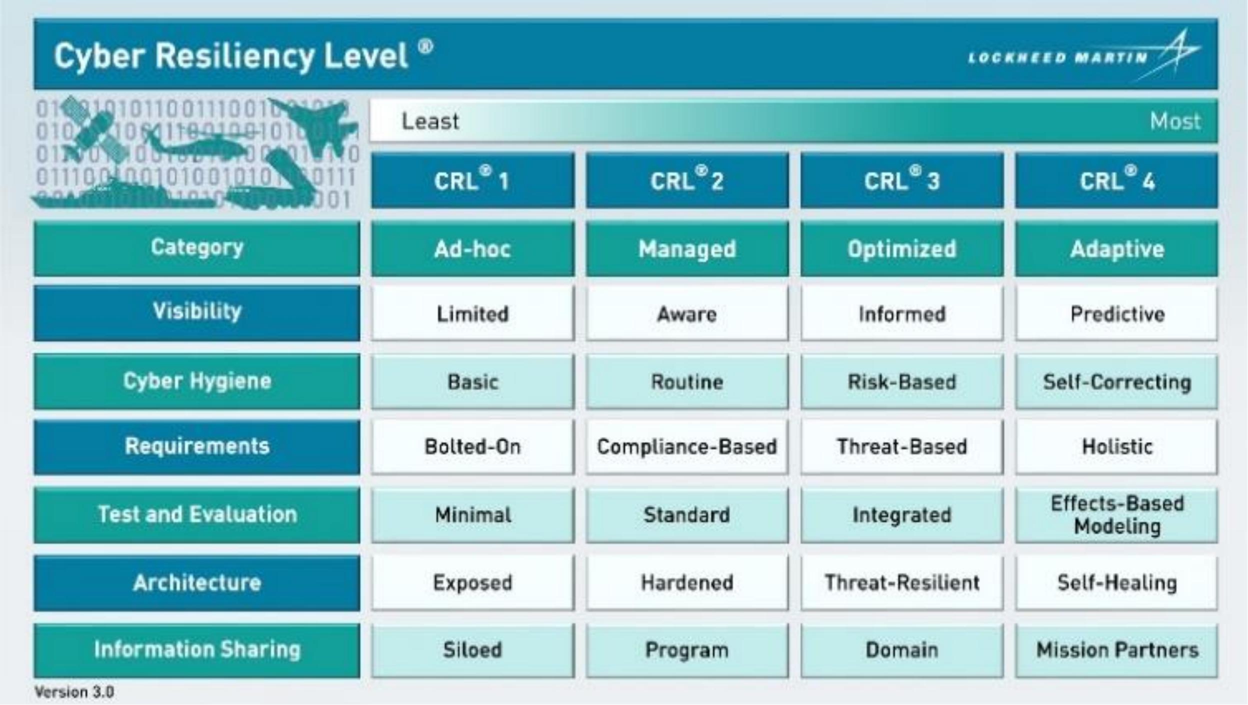
Lockheed Martin

Cyber Resiliency Scoreboard™ (CRS™)

Jacquelyn Blanchard and Orion Strimenos
Lockheed Martin Corporation

From concept through delivery to retirement, Lockheed Martin (LM) integrates full-spectrum cyber solutions into everything we do. LM introduced the Cyber Resiliency Level® (CRL®) framework (see Figure 1Figure 1) in 2019 as the world's first standard method to measure the cyber resiliency maturity of a weapon system[1]. In support of the CRL® framework, LM created the Cyber Resiliency Scoreboard™ (CRS™) tool to assist customers in making informed decisions in selecting courses of action (CoA) and prioritizing their resources for maximum effect against cyber attacks.



Cyber Resiliency Level ®

Least → Most

	CRL® 1	CRL® 2	CRL® 3	CRL® 4
Category	Ad-hoc	Managed	Optimized	Adaptive
Visibility	Limited	Aware	Informed	Predictive
Cyber Hygiene	Basic	Routine	Risk-Based	Self-Correcting
Requirements	Bolted-On	Compliance-Based	Threat-Based	Holistic
Test and Evaluation	Minimal	Standard	Integrated	Effects-Based Modeling
Architecture	Exposed	Hardened	Threat-Resilient	Self-Healing
Information Sharing	Siloed	Program	Domain	Mission Partners

Version 3.0

Figure 1. Cyber Resiliency Level® Framework

Overview

The CRS™ tool captures inputs from subject matter experts (SME) about a system's state of cybersecurity. These inputs are used to calculate key metrics corresponding to each of the six CRL® framework categories: Visibility, Cyber Hygiene, Requirements, Test and Evaluation, Architecture, and Information Sharing[2]. CRS™ consists of a questionnaire and dashboard.

The questionnaire provides qualitative and quantitative cyber performance measures leveraging CRL® category criteria and maturity level descriptions. The questionnaire is divided into four sections:

[1] The term "weapon system" refers to major acquisition programs. These include a broad range of systems such as aircraft, missiles, ships, combat vehicles, sensors, and satellites, as well as their associated ground systems, simulators, and training systems (GAO, 2018).

[2] These six categories form the major recurring concerns of the Department of Defense and were pulled across their strategy, policies, practices, testimonies, and conference proceedings (Beyer, Nance et al., 2020)

Demographics, Differentiation, CRL® Category Evaluations, and Program Strengths and Areas for Improvement. The questionnaire responses are used for back-end analysis and are represented via the dashboard. This analysis provides valuable insight for measuring a system's current level of cyber resiliency and identifying specific opportunities to improve a system's cybersecurity posture.

The dashboard consists of charts and data sets. The CRL® category measurement is calculated, and results are displayed via a radar chart. The radar chart (see Figure 2) provides visualization comparison of measurement data (Nowicki & Merenstein, 2016). Category levels can be measured along their own axis, and overall differences displayed by the size and shape of the polygons. Another advantage of this chart is that the "as-is" and "to-be" measurements can be represented next to each other while still giving each category the same resolution.

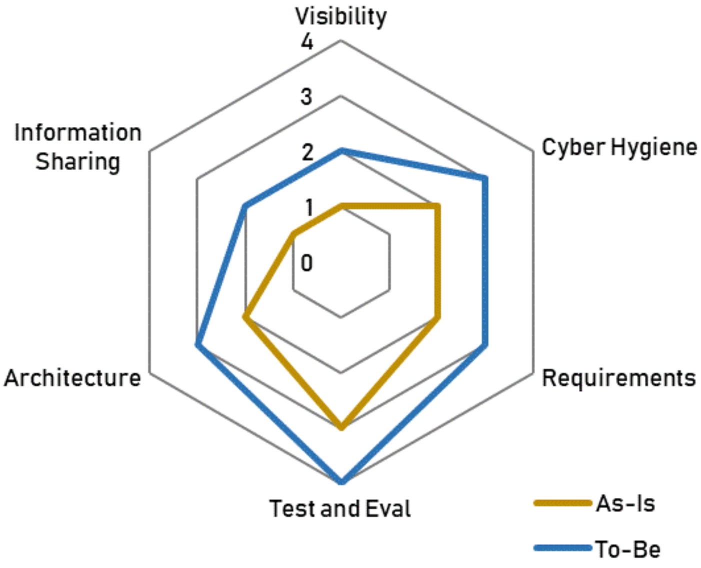
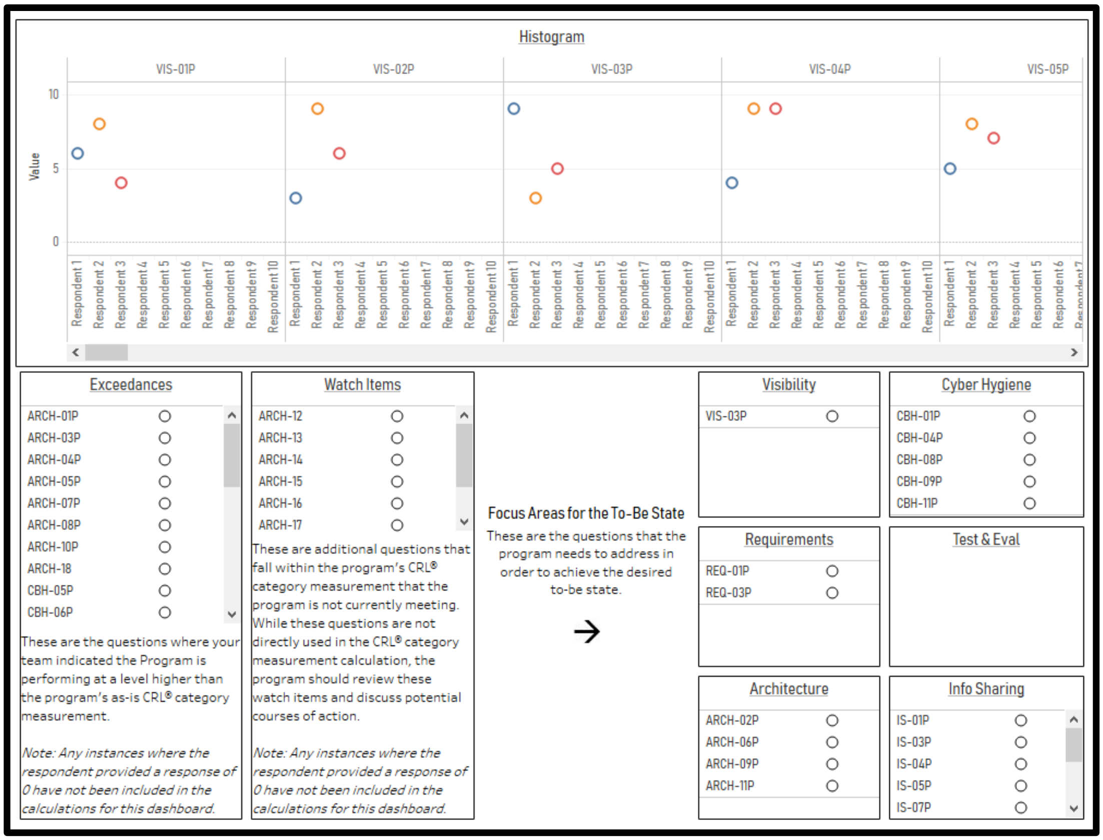


Figure 2: Radar Chart

In addition to the radar chart, program strengths and opportunities to improve the cybersecurity posture of a program are highlighted in individual data sets within the dashboard. The data sets can be leveraged to identify CoAs and investments needed to achieve the "to-be" state of the weapon system.

Usage

The CRL® (2020) whitepaper outlines the recommended process steps programs should follow to use the CRS™ tool. The CRS™ is designed to be completed by three to five cyber SMEs per program. Statistical analysis from program pilots have shown that leveraging three to five cyber SMEs (respondents) when using the CRS™ tool can reduce measurement subjectivity. Once all respondents have completed the questionnaire, the data is exported from the questionnaire tool, processed using statistical analytics, and utilized to create the metrics showcased in the dashboard. One of the dashboard views is showcased in Figure 3 below, and within this view, cyber engineers can analyze the colored circles to easily determine how respondents evaluated each question while the larger boxes in the bottom list areas of exceedances, watch items, and CRL® category "to-be" focus areas. The content displayed in the dashboard was designed to be assessed by cyber SMEs. The program's cyber lead is responsible for summarizing this information and presenting results to program stakeholders.



Exceedances

ARCH-01P ○
ARCH-03P ○
ARCH-04P ○
ARCH-05P ○
ARCH-07P ○
ARCH-08P ○
ARCH-10P ○
ARCH-18 ○
CBH-05P ○
CBH-06P ○

These are the questions where your team indicated the Program is performing at a level higher than the program's as-is CRL® category measurement.

Note: Any instances where the respondent provided a response of 0 have not been included in the calculations for this dashboard.

Watch Items

ARCH-12 ○
ARCH-13 ○
ARCH-14 ○
ARCH-15 ○
ARCH-16 ○
ARCH-17 ○

These are additional questions that fall within the program's CRL® category measurement that the program is not currently meeting. While these questions are not directly used in the CRL® category measurement calculation, the program should review these watch items and discuss potential courses of action.

Note: Any instances where the respondent provided a response of 0 have not been included in the calculations for this dashboard.

Focus Areas for the To-Be State

These are the questions that the program needs to address in order to achieve the desired to-be state.

→

Visibility

VIS-03P ○

Cyber Hygiene

CBH-01P ○
CBH-04P ○
CBH-08P ○
CBH-09P ○
CBH-11P ○

Requirements

REQ-01P ○
REQ-03P ○

Test & Eval

Architecture

ARCH-02P ○
ARCH-06P ○
ARCH-09P ○
ARCH-11P ○

Info Sharing

IS-01P ○
IS-03P ○
IS-04P ○
IS-05P ○
IS-07P ○

Figure 3. Cyber Resiliency Scoreboard™ Dashboard

The CRS™ data, along with risk assessment results, can be leveraged to identify and evaluate candidate CoAs. A cost-benefit analysis should be performed to estimate CoA strengths and weaknesses to determine which CoA will provide the best approach to achieving estimated benefits, preserving cost, and mitigating risks while increasing resiliency. It is recommended that programs complete a CRS™ questionnaire along with a CRL® measurement. For programs with security classification concerns, an offline version is available.

Summary

The LM CRS™ tool measures CRL® category maturity levels of weapon systems. CRS™ allows stakeholders to prioritize and select CoAs to improve cyber resilience. It includes a questionnaire and dashboard. The tool can be used in any phase of the acquisition lifecycle.

CRS™ is easily adaptable and has been successfully applied to numerous programs across each of our business areas. Feedback from programs is used to validate CRL® category criteria, determine metrics and data representation, and improve tool performance. Program feedback is also leveraged to streamline the measurement process, making it more simplistic, understandable, and easier to discuss results with stakeholders. To learn more about CRL®, visit lockheedmartin.com/crl.

CRS™ is a proven tool in mitigating risks and performing cost-benefit analysis for determining which mitigations provide the most cost-effective benefits. To learn more about CRS™, visit lockheedmartin.com/crs.

Acknowledgements

David Harrison, Ethan Puchaty, Shaun Thomas, Dr. Dawn Beyer, Judy Lim, and Jason Bacheler provided significant contribution to the work presented in this paper.

References

Beyer, D., Nance, M., Lardieri, P., Roberts, N., Hale, R., Plummer, T., Johnson II, J. (2020). *Lockheed Martin Cyber Resiliency Level® (CRL®) Framework V3.0 for Weapon, Mission, and Training Systems.* https://lockheedmartin.com/crl

GAO. (2018). *GAO-19-128: Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities.* https://www.gao.gov/products/GAO-19-128

Nowicki, H., Merenstein, C. (2016). Radar Chart: CS 465: *Information Visualization – Spring 2016*. https://www.cs.middlebury.edu/~candrews/showcase/infovis_techniques_s16/radar_chart/